

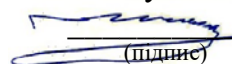
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»

Факультет електроніки
(повна назва інституту/факультету)

Кафедра акустичних та мультимедійних електронних систем
(повна назва кафедри)

«До захисту допущено»

Завідувач кафедри


(підпис)

С.А. Найда
(ініціали, прізвище)

“01” червня 2020 р.

Дипломна робота

на здобуття ступеня бакалавра

зі спеціальності(спеціалізації) 171 Електроніка («Електронні та інформаційні системи і технології телебачення, кінематографії та звукотехніки»)

(код і назва)

на тему: «Дослідження надійності безпроводових технологій у системі розумний будинок»

Виконав: студент IV курсу, групи ДВ-61
(шифр групи)

Зінченко Дмитро Володимирович

(прізвище, ім'я, по батькові)



(підпис)

Керівник

доцент, к.т.н., доцент Лазебний В.С.

(посада, науковий ступінь, вчене звання, прізвище та ініціали)



(підпис)

Консультант

(назва розділу) (посада, вчене звання, науковий ступінь, прізвище, ініціали)

(підпис)

Рецензент доцент каф. ЕПС, доцент, к.т.н. Михайлов С.Р.

(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище, ініціали)



(підпис)

Засвідчую, що у цьому дипломному проєкті немає запозичень з праць інших авторів без відповідних посилань.

Студент



(підпис)

Київ – 2020 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Факультет Електроніки

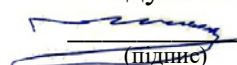
Кафедра акустичних та мультимедійних електронних систем

Рівень вищої освіти – перший (бакалаврський)

Спеціальність(спеціалізації)171 Електроніка(«Електронні та інформаційні системи і технології телебачення, кінематографії та звукотехніки»)

ЗАТВЕРДЖУЮ

Завідувач кафедри


(підпис)

С.А. Найда
(ініціали, прізвище)

«25» травня 2020 р.

ЗАВДАННЯ
на дипломну роботу студенту

Зінченку Дмитру Володимировичу
(прізвище, ім'я, по батькові)

1 Тема роботи: «Дослідження надійності безпроводових технологій у системі розумний будинок»

керівник роботи Лазебний Володимир Семенович, к.т.н., доц.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «25»травня 2020 р. №1196-с

2 Термін подання студентом роботи 04 червня 2020 р.

3 Вхідні дані до роботи: 1) Протокол Wi-Fi; 2)Протокол ZigBEE; 3) протокол BLE 4) Протокол Thread; 5) Протокол Z-Wave6) Модель OSIдля аналізу технологій.

4 Зміст дипломної роботи: 1)Розглянути основні вимоги та стандарти для системи розумний будинок; 2)Розглянути архітектури та основні технічні особливості кожної технології; 3)Дослідити надійність протоколів обміну інформацією із застосуванням моделі OSI; 4)Виявити переваги та недолікикожної конкретної технології.

5 Перелік ілюстративного матеріалу: комплект презентації за матеріалами проведеного дослідження.

6. Консультанти розділів роботи


Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 11 березня 2020 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Пошук і опрацювання матеріалів за темою дисертації	24.03.2020	виконано
2	Дослідження протоколів обміну інформацією	20.04.2020	виконано
3	Написання третього розділу	10.05.2020	виконано
4	Підготовка матеріалів до друку та оформлення пояснювальної записки	30.05.2020	виконано
5	Підготовка та оформлення презентації для доповіді	1.06.2020	виконано


Студент


(підпис)

Дмитро ЗІНЧЕНКО

(ініціали, прізвище)

Керівник роботи


(підпис)

Володимир ЛАЗЕБНИЙ

(ініціали, прізвище)

РЕФЕРАТ

Дипломна робота: 69 с., 4 рис., 5 табл., 1 додаток, 17 джерел.

РОЗУМНИЙ БУДИНОК, ПРОТОКОЛ, МОДЕЛЬ OSI, ІНТЕРЕНЕТ РЕЧЕЙ, БЕЗПРОВОДОВІ, ДОМАШНЯ АВТОМАТИЗАЦІЯ, СТАНДАРТ, ТЕХНОЛОГІЯ, ПЕРЕВАГИ, НЕДОЛІКИ, ZIGBEE, BLUETOOTH LOW ENERGY, Z-WAVE, THREAD, WI-FI.

Метою роботи є дослідити надійність безпроводових технологій, які застосовують для реалізації систем «розумний будинок». Визначити проблемні місця, з'ясувати можливість удосконалити технології передавання даних для системи SmartHome.

Об'єктом дослідження є технології та стандарти безпроводових мереж системи «Розумного будинку».

Предметом дослідження є «Розумний будинок» як цілісна та надійна система.

Новизна роботи полягає в узагальненні наявної інформації стосовно організації та особливостей функціонування безпроводових технологій і розроблені рекомендації щодо обрання найвигіднішої та найнадійнішої для застосування у системі «Розумний будинок»

Результатом дипломної роботи є узагальнення світового досвіду стосовно розвитку сучасних безпроводових технологій, формування порівняльних характеристик різних протоколів системи домашньої автоматизації, з'ясування позитивних та негативних властивостей протоколів а також їх архітектури.

ABSTRACT

The object of research is the technologies and standards of wireless networks of the Smart Home system.

The subject of the study is "Smart Home" as a holistic and reliable system.

The novelty of the work is to summarize the available information on the organization and features of wireless technologies and developed recommendations for choosing the most profitable and most reliable for use in the system "Smart Home"

The result of the thesis is the generalization of world experience in the development of modern wireless technologies, the formation of comparative characteristics of different protocols of home automation system, clarifying the positive and negative properties of protocols and their architecture.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ	8
ВСТУП.....	9
1 ОСНОВНІ ВМОГИ ТА СТАНДАРТИ СИСТЕМИ РОЗУМНИЙ БУДИНОК.11	11
1.1 Енергоживлення	11
1.2 Радіус дії і безпека	11
1.3 Можливість роботи за розкладом і без нього	12
1.4 Відмовостійкість	12
1.5 Взаємна сумісність.....	13
1.6 Модель OSI.....	14
2 АРХІТЕКТУРА ТА ТЕХНІЧНІ ОСОБЛИВОСТІ БЕЗПРОВОДОВИХ ТЕХНОЛОГІЙ ДОМАШНЬОЇ АВТОМАТИЗАЦІЇ	16
2.1.Застосування технології Wi-Fi у SmartHome.....	16
2.1.1 Введення	16
2.1.2 Принцип технології WiFi.....	16
2.1.3 Загальна конструкція системи.....	17
2.1.4 Розробка програмного забезпечення системи	18
2. 2 ТехнологіяZigBee	19
2.2.1 Загальні відомості технології	19
2.2.2 ZigBeeархітектура	19
2.2.3 Режими роботи Zigbee та його топології	21
2.2.4 Застосування технології Zigbee.....	22
2.3 Технологія Z-Wave.....	23
2.3.1 Z-Wave: Mesh - мережа	23
2.3.2 Z-WaveAlliance	24
2.3.3 ФінкціонуванняZ-Wave	24
2.3.4 Z-Wave: Основні характеристики	25
2.4 Технологія BluetoothLowEnergy.....	26
2.4.1 Найнижче енергоспоживання.....	27

2.4.2 Сумісність.....	28
2.4.3 Співіснування безпроводових стандартів.....	28
2.4.4 Дальність зв'язку	29
2.4.5 Простота використання та інтеграції	29
2.4.6 Технічні подробиці.....	29
2.5 Технологія Thread.....	30
2.5.1 Топологія мережі Thread.....	32
2.5.2 Взаємодія з IP-мережами	33
3 ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ НА ОСНОВІ МОДЕЛІ OSI	35
3.1 Дослідження технології Wi-Fi	35
3.1.1 Переваги Wi-Fi як протоколу домашньої автоматизації.....	35
3.1.2 Недоліки Wi-Fi як протоколу домашньої автоматизації.....	36
3.2 Z-Wave згідно моделі OSI.....	39
3.2.1 Переваги Z-Wave.....	42
3.2.2 Недоліки Z-Wave.....	45
3.3 ZigBee в рамках моделі OSI.....	46
3.3.1 Переваги ZigBee	47
3.3.2 Недоліки ZigBee	49
3.4 Протокол Thread в моделі OSI.....	52
3.4.1 Переваги протоколу розумного будинку Thread	53
3.4.2 Недоліки технології Thread.....	53
3.5 Bluetooth Low Energy в моделі OSI	56
3.5.1 Переваги Bluetooth Low Energy	57
3.5.2 Недоліки технології Bluetooth Low Energy	58
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ.....	63
ДОДАТОК А	65

ПЕРЕЛІК СКОРОЧЕНЬ

AES	– Advanced Encryption;
IEEE	– Institute of Electrical and Electronics Engineers;
OSI	– The Open Systems Interconnection model;
IP	– Internet Protocol;
6LoWPAN	– IPv6 over Low power Wireless Personal Area Networks;
IPv6	– Internet Protocol version 6;
Wi-Fi	– Wireless Fidelity;
USB	– Universal Serial Bus;
SIG	– Special Interest Group;
BLE	– Bluetooth Low Energy;
IoT	– Internet of Things;
UHF	– Ultra high frequency;
SHF	– Super high frequency;
ISM	– Industrial, scientific and medical;
WPAN	– Wireless personal area network;
MAC	– Media Access Control;
CSMA	– Carrier Sense Multiple Acces;
LAN	– Local Area Network;
ANT	– Adaptive Network Topology;
TCP	– Transmission Control Protocol;
CCM	– Counter Mode with Cipher Block Chaining Message Authentication Code;

ВСТУП

Розумний дім сьогодні стає реальністю. Це автоматизований дім із пристроями, які сполучені один з одним і якими можна керувати на домашній панелі приладів або за допомогою смартфона через Інтернет. Але до недавнього часу SmartHome завжди залишався високим ринком або був майданчиком для кількох любителів та ранніх новаторів.

Потенціал домашньої автоматизації на масовому ринку визнаний давно, і нарешті сьогодні ми спостерігаємо початок тієї нової ери, коли багато великих операторів, постачальників послуг та комунальних служб запускають програми SmartHome. Їм можна керувати через пристрій телевізора або шлюз через Інтернет, що дозволяє абонентам перетворювати свої будинки у найсучасніші машини, за якими можна відстежувати та контролювати з будь-якої точки світу за допомогою смартфонів, планшетів або мобільних пристроїв.

Оператори починають пропонувати додатки SmartHome як додаткову послугу до своїх поточних пропозицій телебачення, телефонних послуг, Інтернету та розваг; їх клієнти можуть вибирати з додатків, що відповідають їх конкретним потребам. Власник одного будинку має різні вимоги зробити його будинок розумнішим, ніж люди похилого віку або сім'я з дітьми. Ці програми можуть перевіряти та керувати «речами вдома», такими як контроль температури (зміна налаштування термостата), безпека (переконайтесь, що двері заблоковані), сигналізація (датчики та камери) або управління енергією (наприклад, управління освітленням) та моніторинг стану здоров'я та стану літніх людей. Щоб усі ці різні програми були сумісними, всі вони повинні мати можливість взаємодіяти один з одним.

Актуальність теми обумовлено бурхливим розвитком систем «Розумного будинку» та великою кількістю проводових та безпроводових технологій для обміну даними в таких системах.

Метою роботи є дослідити надійність безпроводових технологій, які застосовують для реалізації систем «розумний будинок». Визначити проблемні

місця, з'ясувати можливість удосконалити технології передавання даних для системи SmartHome.

Для досягнення поставленої мети необхідно виконати такі завдання:

- проаналізувати найбільш вживані безпроводові технології
- детально розглянути кожну технологію
- проаналізувати програмне забезпечення та дослідити сумісність між іншими пристроями
- проаналізувати наскільки сучасні проблеми вже вирішені

Методом дослідження критичний аналіз для з'ясування характеристик та особливостей застосування, порівняльний аналіз наявних систем.

Об'єктом дослідження є технології та стандарти безпроводових мереж системи Розумного будинку.

Предметом дослідження система «Розумний будинок»

Новизна роботи полягає в узагальненні наявної інформації стосовно організації та особливостей функціонування безпроводових технологій і розроблені рекомендація щодо використання та планування подібних технологій.

Практична цінність. Результати роботи будуть корисними для фахівців, що працюють у сфері Інтернет зв'язку і систем доступу до інформаційних ресурсів. Результати можна використати під час планування та введення в експлуатацію мереж віддаленого доступу та внутрішнього доступу, а також у навчальному процесі під час підготовки фахівців у сфері електроніки.

1 ОСНОВНІ ВМОГИ ТА СТАНДАРТИ СИСТЕМИ РОЗУМНИЙ БУДИНОК

Перш за все давайте розберемося, власне, що це за протоколи зв'язку і яка їхня роль в тому, щоб наші оселі ставали розумними. Протокол -це комплект правил, які дають можливість двом або ж більше приладам в мережі ввести надійну асоціацію і благополучно обмінюватися даними один з одним. Для того щоб розумний будинок став реальністю, велика частка комунікацій має бути безпроводовою.

1.1 Енергоживлення

За останні роки був помічений розмашистий діапазон технологій для організації безпроводового зв'язку між приладами. У переважній більшості випадків вони підкоряються надзвичайно строгим вимогам щодо споживання енергії та пропускнуої можливості. Ці чинники важливо нарощують час роботи від батареї і дають можливість застосувати більшу кількість приладів в обмеженому місці розумного житла або ж кабінету. Дешевий для домашньої автоматизації радіочастотний діапазон обмежений. В наслідок цього для одночасної роботи великої кількості приладів надзвичайно принципово поліпшити його впровадження будь-яким цим пристроєм.

Цим чином, досконалий девайс для розумного житла зобов'язаний застосувати безпроводовий приймач і передавач, які споживають малу чисельність енергії, щоб прилад міг працювати безлічі місяців або ж в тому числі і років без потреби заміни батареї. Критерії безпроводового протоколу зв'язку споживаної потужності приладами розумного житла зобов'язані бути досить суворими.

1.2 Радіус дії і безпека

Сигнал від всякого вашого девайса зобов'язаний розмірено і з малою затримкою досягати будь-якого іншого розумного приладу, встановленого в

найвіддаленішій ділянці житла. Лампочки, які підключаються з затримкою кілька секунд, або ж розумний замок, не відразу пускає вас всередину - це не те, з чим у нас асоціюється нинішній розумний будинок. Не кажучи вже про датчики задимленості, протікання газу, які мають включатися виразно і швидко. В наслідок цього сигнали від всякого вашого приладу зобов'язані долати всілякі завади, поширюватися крізь стінки і підлоги житла. Всі розумні девайси зобов'язані працювати як єдиний узгоджений пристрій. І, звичайно ж, завади від інших безпроводових мереж або ж інших приладів, що працюють на тій же частоті, зобов'язані бути усунені або ж зведені до мінімуму.

1.3 Можливість роботи за розкладом і без нього

Програмний функціонал, реалізований для деяких відомих безпроводових технологій домашньої автоматизації, дозволяє задати розклад для цих заходів, як, наприклад, вихід жалюзі, підключення світла або ж опалення. Але майже всі дії, що відбуваються в нашому розумному житлі, неможливо спланувати заздалегідь. Протікання води, витік газу, виникнення диму або ж злом не можна передбачати. А детектори температури, вимикачі, диммери, шаттер і т. Д. Не всякий раз можливо запрограмувати на виконання автоматичних сценаріїв. В наслідок цього ще важливо, щоб будь-який IoT-пристрій в розумному житлі міг вислати або ж отримати команду на виконання тих або ж інших вчинків не за сценарієм, а в залежності від ситуації.

1.4 Відмовостійкість

Топологія безпроводової мережі, яку підтримує той або ж інший протокол розумного житла, містить вирішальне значення для такого актуального чинника, як відмовостійкість. Крім того, вона робить прямий вплив на вже згадані нами заощадження енергії і радіус дії приладу. Нинішній погляд на зведення безпроводових мереж господарської автоматизації передбачає децентралізований

розклад, який користується топологією мережі (mesh-мережі). Будь-який прилад в подібній мережі має можливість безпосередньо зв'язуватися з будь-яким іншим пристроєм в радіусі власного впливу. У разі якщо два прилади дуже далеко один від одного, то сигнали можуть переходити крізь проміжні прилади даної мережі, таким чином важливо зростає зона впливу приладів.

Крім такого, нові девайси можуть додаватися, а старі видалятися без несприятливого впливу на надійність мережі. Втім для більшості пористих сіток ще потрібен «основний» прилад, який працює мережевим контролером для координації спільної роботи десятків або ж в тому числі і сотень приладів в одній мережі. У разі якщо провідний прилад виходить з ладу, то іншому приладу слід вміти механічно брати на себе управління мережею. Ця властивість mesh-мереж містить вирішальне значення для забезпечення незмінної безперебійної роботи всієї системи.

1.5 Взаємна сумісність

І, врешті-решт, на самому базовому рівні думка господарської автоматизації полягає в тому, власне що всі наші мудрі прилади зобов'язані зливатися в мережу і «спілкуватися» один з одним. Втім дійсність ще далека від даної досконалої концепції. Мова поки ж в тому числі і не йде про забезпечення порівнянності різних стереотипів безпроводових протоколів зв'язку, яка дозволяла б приладам і системам взаємодіяти один з одним. Питання полягає в сумісності в рамках 1-го еталона. Легше кажучи, далеко не кожна розробка, яку ви виберете в якості ключової для домашньої автоматизації, має можливість забезпечувати що різні розумні продукти стануть «розуміти» один одного. В даний момент, наприклад, може виявитися, що коли при задимленні датчик диму вислав звістку керуючому пристрою, ви зможете не отримати попередження про загрозу. Перша причина в тому, власне, що датчик і контроллер, хоч і засновані на одному стандарті, але випущені різними виробниками, можуть «не зрозуміти» один одного.

Чому це відбувається? Питання сумісності - це не проблема мережевих протоколів, що забезпечують включення. Неочевидні з першого погляду, але від

того не менш неабиякі труднощі заховані глибше, і полягають в недоступності нормальних форматів даних або ж сукупних програмних інтерфейсів.

1.6 Модель OSI

Різні технології безпроводового зв'язку розроблялися для виконання різних завдань. Відповідно до цього, і власну роботу вони роблять по-різному. Майже всі нюанси будуть безперечними, в разі якщо розглянути ці мережеві технології через призму еталонної моделі OSI.

Міжнародна організація по стандартизації (International Organization for Standardization, ISO) придумала модель взаємодії розкритих систем (Open Systems Interconnection, OSI) ще в 80-х роках минулого століття. OSI - база для координації розробки стереотипів зв'язку і до сих пір залишається еталонною моделлю для комунікаційних мереж. Конструкція OSI оцінює процес комунікацій в мережі як керовану ієрархію, що складається з 7 значень. Кожен з них відповідає за конкретні функції і постановляє виразно конкретні завдання в рамках 1-го значення, а ще взаємодії з рівнями, розташованими саме нижче і вище. Еталонна модель OSI виглядає наступним чином:

- Прикладний рівень (Application).
- Рівень представлення (Presentation).
- Сеансовий рівень (Session).
- Транспортний рівень (Transport).
- Мережевий рівень (Network).
- Канальний рівень (DataLink).
- Фізичний рівень (Physical).

При більш детальному розгляді будь-якої певної безпроводової технології домашньої автоматизації ми станемо заперечувати до даної моделі, щоб

продемонструвати, на яких рівнях і в який спосіб працює будь-який протокол зв'язку, і що це означає для кінцевих користувачів.

Кожен з цих рівнів важливий, наприклад як визначає завдання, які вважаються обов'язковою частиною процесу комунікацій між приладами розумного житла.

Верхній - прикладний рівень вважається ключем до порівнянності приладів. У разі якщо прикладний рівень не визначений стандартом, прилади різних виробників елементарно не зможуть "зрозуміти" один одного. Даний нюанс роз'яснює, чому проблема сумісності є не тільки лише в ситуаціях, коли 2 прилади, що використовують різні протоколи, не мають шанси обмінюватися даними.

Висновки

На даний момент існує дуже багато протоколів зв'язку для домашньої автоматизації. При виборі протоколу слід звернути увагу на такі властивості протоколів, як:

- електроживлення
- радіус дії та безпека
- можливість роботи за розкладом та без нього
- відмовостійкість
- взаємна сумісність

А також для більш детального розгляду протоколів, можна проаналізувати конкретно кожний за моделлю OSI.

2 АРХІТЕКТУРА ТА ТЕХНІЧНІ ОСОБЛИВОСТІ БЕЗПРОВОДОВИХ ТЕХНОЛОГІЙ ДОМАШНЬОЇ АВТОМАТИЗАЦІЇ

2.1.Застосування технології Wi-Fi у SmartHome

2.1.1 Введення

Завдяки постійному вдосконаленню технологій людям комфортніше жити в домашніх умовах та зручніше і безпечніше.

В даний час тенденція розвитку розумного будинку - від централізованого контролю до розподіленого контролю. Наразі використовуються чотири основні безпроводові технології в розумному будинку: Bluetooth, WiFi, Z-Wave, Zig-bee. Найбільш конкурентоспроможною є технологія WiFi та Zig-bee.

Розглянемо систему управління розумним будинком, засновану на WiFi.

2.1.2 Принцип технології WiFi

Повна назва WiFi - WirelessFidelity, це специфікація безпроводової мережі 802.11b та технологія безпроводової передачі короткого діапазону, яка спрямована на поліпшення сумісності безпроводового зв'язку. Мережеві продукти на основі стандарту IEEE802.11. WiFi зазвичай використовують 2,4G UHF або 5G SHF ISM діапазони. З'єднання безпроводової локальної мережі зазвичай захищені паролем, але вони також можуть бути відкритими, без паролів і можуть бути підключені пристрої для всієї мережі.

Принцип роботи системи управління розумним будинком, заснованої на WiFi, полягає в тому, що є безліч безпроводових смарт вузлів, які утворюють мережу домашньої області, кожен розумний підвузол включає модуль прийому WiFi та домашній шлюз також має безпроводовий модуль передачі WiFi.

Перевагами WiFi є те, що технологія охоплює широку територію і має велику ефективну відстань. Відстань спілкування на відкритому повітрі до 305м, а відстань зв'язку в закритій місцевості становить 76-122м. Це може бути застосовується не лише до місцевих приміщень, а й до всіх будівель.

Швидкість передачі дуже швидка, до 54 Мбіт / с. Крім низької вартості, вона має низьку потужність споживання. Вплив випромінювання, що виробляється Wi-Fi на організм людини, незначне в безпечних межах. Однак, оскільки Wi-Fi використовує радіочастотну технологію, повітря використовується як середовище для передачі та прийому даних,

Сигнали, що передаються через радіохвилі, легко порушуються зовнішнім середовищем та безпека не висока, тому вони не підходять для систем управління розумними будинками, які потребують високої безпеки.

2.1.3 Загальна конструкція системи

За платформу обирається система Android, система включає процесор, модуль Wi-Fi, смарт-телефон як термінал управління та інтелектуальна система управління. Інтелектуальна система управління включає в себе інтелектуальну систему управління освітленням, інтелектуальну систему управління аудіовізуальним обладнанням, система моніторингу відео в режимі реального часу, а також, систему Android смартфонів через мережу Wi-Fi для досягнення мети контролю побутової техніки. Функція цієї системи полягає в тому, щоб через управління смартфоном надіслати команду управління до процесора мережі Wi-Fi. Процесор отримує команду і аналізує її, щоб віддалено встановити двері, кондиціонер, контрольний зонд і світло. Користувачі також можуть використовувати смартфон для збору даних у режимі реального часу, які надсилаються центральним процесором. Апаратна платформа є важливою частиною визначення продуктивності та стабільності системи. Модуль Wi-Fi, смарт-телефон на базі системи Android як терміналу управління.

Термінал управління передає інформацію до модуля Wi-Fi, підключеного до цієї ж мережі через Wi-Fi. Модуль Wi-Fi передає отриманий сигнал до процесора через послідовний порт і процесор реалізує контроль над побутовим приладом відповідно до отриманих інструкцій. Загальна структура системи показана на рисунку 1.

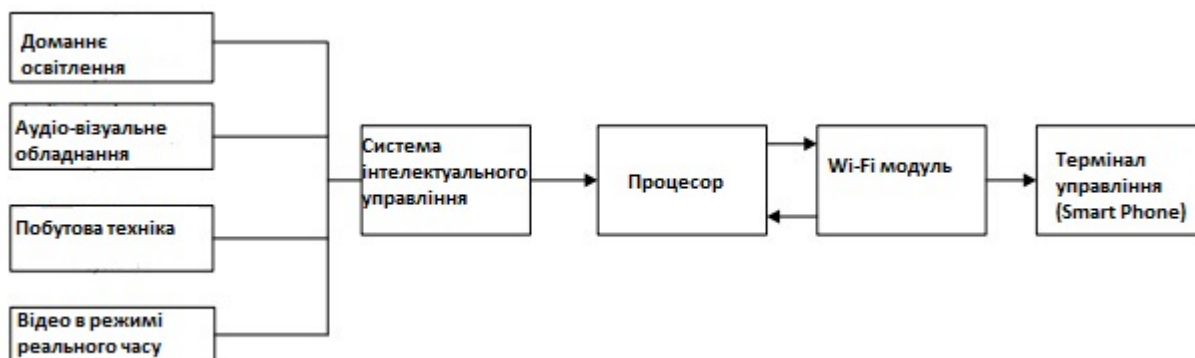


Рисунок 2.1 – Загальна структурна схема системи

2.1.4 Розробка програмного забезпечення системи

Розробка програмного забезпечення системи базується на системі Android над системою Linux.

Операційна система з високим ступенем свободи, відкритості, широким спектром застосувань, і має чудовий потенціал для розвитку, вона також є дуже конкурентоспроможною у майбутньому. Android- операційна система, як платформа для розвитку інтелектуальної системи управління будинком.

Встановивши додаток (Інтерфейс на смартфоні), користувач може реалізувати управління комутацією побутової техніки, централізоване управління освітленням будинку та моніторинг домашньої ситуації в реальному часі, можна керувати електрообладнанням будинку не тільки централізовано, також можна реалізувати віддалене управління, зменшити потенційну небезпеку та по-справжньому застосувати сучасну передову технологію до життя людей.

По-перше, користувачеві необхідно зареєструвати обліковий запис у APP, встановити пароль та увійти в основний інтерфейс управління через зареєстрований обліковий запис для забезпечення конфіденційності користувача. Основний інтерфейс містить інтерфейс налаштувань, в якому ви можете встановити тон комутатора, стиль інтерфейсу тощо. Це може збільшити досвід та персоналізацію користувачів.

Інтерфейс домашнього управління має чотири підмодулі: інтерфейс управління розумними побутовими приладами розумного дому, Інтерфейс управління освітленням, інтерфейс управління аудіо- та відеоапаратурою, інтерфейс відеоспостереження.

2. 2 Технологія ZigBee

2.2.1 Загальні відомості технології

Зв'язок Zigbee спеціально побудований для мереж управління та датчиків за стандартом IEEE 802.15.4 для безпроводових персональних мереж (WPAN), і це продукт від альянсу Zigbee. Цей стандарт зв'язку визначає фізичні та контрольні рівні доступу до засобів масової інформації (MAC) для обробки багатьох пристроїв із низькою швидкістю передачі даних. Ці ZigBee WPAN працюють на частотах 868 МГц, 902-928 МГц і 2,4 ГГц. Швидкість даних 250 кбіт / с найкраще підходить для періодичної, а також проміжної двосторонньої передачі даних між датчиками та контролерами.

Zigbee - це недорога і малопотужна сітчаста мережа, широко розгорнута для контролю та моніторингу програм, де вона охоплює 10-100 метрів у межах дальності. Ця система зв'язку дешевша і простіша за інші фірмові безпроводові сенсорні мережі, такі як Bluetooth та Wi-Fi.

Zigbee може працювати в різних режимах, внаслідок чого енергія акумулятора зберігається. Мережі Zigbee розширюються із застосуванням маршрутизаторів і дозволяють багатьом вузлам з'єднуватися між собою для побудови мережі більш широкої площі.

2.2.2 ZigBee архітектура

Структура системи Zigbee складається з трьох різних типів пристроїв, таких як Zigbee координатор, маршрутизатор та кінцевий пристрій. Кожна мережа Zigbee повинна складатися щонайменше з одного координатора, який виконує функції

кореня та мосту мережі. Координатор несе відповідальність за обробку та зберігання інформації під час виконання операцій прийому та передачі даних. Маршрутизатори Zigbee виконують роль посередницьких пристроїв, які дозволяють передавати дані та повертатися через них на інші пристрої. Кінцеві пристрої мають обмежену функціональність для зв'язку з батьківськими вузлами, таким чином, щоб енергія акумулятора зберігалася, як показано на малюнку. Кількість маршрутизаторів, координаторів та кінцевих пристроїв залежить від типу мережі, наприклад мереж зірок, дерев та сіток.

Архітектура протоколів Zigbee складається з стеку різних шарів, де IEEE 802.15.4 визначається фізичним та MAC-шарами, тоді як цей протокол завершується накопиченням власних мережесхем та прикладних рівнів Zigbee.

- Фізичний шар (Physical (PHY) Layer): Цей шар виконує операції з модуляції та демодуляції відповідно до передачі та прийому сигналів. MACLayer: Цей рівень відповідає за надійну передачу даних шляхом доступу до різних мереж з уникненням зіткнень з множинним доступом носія даних (CSMA). Цей шар передає маякові кадри для синхронізації зв'язку.
- Мережесхема шар (NWKLayer) : Цей рівень забезпечує всі операції, пов'язані з мережею, такі як налаштування мережі, підключення кінцевого пристрою та відключення до мережі, маршрутизація, конфігурація пристрою тощо.
- Підшар підтримки додатків ((APS) Sub-Layer) : Цей рівень дозволяє службам, необхідним для об'єкта та прикладних пристроїв Zigbee, взаємодіяти з мережесхемними рівнями для служб управління даними. Цей рівень відповідає за відповідність двох пристроїв відповідно до їхніх послуг та потреб.
- Прикладні рамки (ApplicationFramework) : надає два типи даних, як пара ключових значень, так і загальні послуги повідомлень. Загальне повідомлення - це структура, визначена розробником, тоді як пара ключових значень використовується для отримання атрибутів всередині об'єктів програми. ZDO забезпечує інтерфейс між об'єктами програми та шаром APS в пристроях

Zigbee. Він відповідає за виявлення, ініціювання та прив'язку інших пристроїв до мережі.

2.2.3 Режими роботи Zigbee та його топології

Двостороння передача даних Zigbee передається у двох режимах: у режимі без маяка та режимі маяка. У режимі маяку координатори та маршрутизатори постійно контролюють активний стан вхідних даних, завдяки чому витрачається більше енергії. У цьому режимі маршрутизатори та координатори не сплять, оскільки в будь-який час будь-який вузол може прокинутися та спілкуватися. Однак для цього потрібне більше джерела живлення, а загальне споживання електроенергії є низьким, оскільки більшість пристроїв тривалий час перебувають у неактивному стані в мережі.

У режимі маяка, коли немає зв'язку з кінцевими пристроями, маршрутизатори та координатори переходять у стан сну. Періодично цей координатор прокидається і передає маяки маршрутизаторам в мережі. Ці маякові мережі працюють для часових інтервалів, а значить, вони працюють, коли потрібна комунікація, це призводить до менших циклів роботи та більшого використання акумулятора. Ці режими радіомаяка та не маяка Zigbee може керувати періодичними (датчики даних), переривчастими (вимикачі світла) та повторюваними типами даних.

Zigbeepідтримує декілька мережевих топологій; Однак найбільш часто використовувані конфігурації - це зірки, сітки та топології дерев кластера. Будь-яка топологія складається з одного або декількох координаторів. У зірковій топології мережа складається з одного координатора, який відповідає за ініціювання та керування пристроями по мережі. Усі інші пристрої називаються кінцевими пристроями, які безпосередньо спілкуються з координатором. Це застосовується в галузях, де всі пристрої кінцевих точок потрібні для зв'язку з центральним контролером, і ця топологія проста і зручна для розгортання.

У сітчастих і деревних топологіях мережа Zigbee розширена кількома маршрутизаторами, де координатор відповідає за їх огляд. Ці структури дозволяють

будь-якому пристрою спілкуватися з будь-яким іншим суміжним вузлом для забезпечення надмірності даних. Якщо який-небудь вузол виходить з ладу, інформація спрямовується автоматично на іншій пристрій цими топологіями. Оскільки надлишок є головним фактором у галузях промисловості, отже, переважно використовується сітчаста топологія. У мережі дерев кластерів кожен кластер складається з координатора з вузлами листків, і ці координатори з'єднані з батьківським координатором, який ініціює всю мережу.

Завдяки таким перевагам технології Zigbee, як низька вартість та низькі енергоресурси роботи та її топології, ця технологія зв'язку невеликого діапазону найкраще підходить для декількох застосувань порівняно з іншими власними комунікаціями, такими як Bluetooth, Wi-Fi тощо.

2.2.4 Застосування технології Zigbee

Промислова автоматизація: у виробничій галузі комунікаційний зв'язок постійно контролює різні параметри та критичне обладнання. Отже, Zigbee значно знижує цю вартість зв'язку, а також оптимізує процес управління для більшої надійності.

Домашня автоматизація: Zigbee ідеально підходить для дистанційного керування побутовою технікою як управління системою освітлення, керуванням приладами, керуванням системою опалення та охолодження, експлуатацією обладнання безпеки та управлінням, спостереженням тощо.

Інтелектуальне вимірювання: віддалені операції Zigbee при інтелектуальному вимірюванні включають реакцію на споживання енергії, підтримку цін, безпеку крадіжок електроенергії тощо.

Операції Zigbee включають дистанційний моніторинг температури, пошук несправностей, управління реактивною потужністю тощо.

2.3 Технологія Z-Wave

Z-Wave - це безпроводовий протокол, що використовує радіохвилі низької енергії, щоб допомогти розумним пристроям успішно контактувати один з одним.

Компанія Zensys з Данії розробила Z-Wave у 2001 році. Зазначена мета полягала у створенні економічно вигідної альтернативи Zigbee, яка б давала змогу пристроям різних марок взаємодіяти в гармонії.

Випущена в 2004 році, Z-Wave вийшла на масовий ринок у 2005 році, утворивши Альянс Z-Wave.

Z-Wave працює, використовуючи дуже мало енергії. Використовуючи частоти 908,42 МГц у США та 868,42 МГц по всій Європі, Z-Wave страждає від дуже невеликих завад, оскільки діапазон 800 - 900 добре очищає частоти 2,4 ГГц і 5 ГГц, які використовуються WiFi та іншими пристроями, приладами та протоколами.

Безпроводова мережева мережа Z-Wave може підтримувати до 232 пристроїв. Хоча це практична межа, після 40 або 50 пристроїв матимуть невеликі затори.

Щоб зрозуміти, як працює Z-Wave, потрібно чітко ознайомитись із сітчастими мережами та перевагами, які вони надають.

2.3.1 Z-Wave: Mesh - мережа

У стандартних радіочастотних мережах більша кількість пристроїв призводять до проблемних перевантажень.

Mesh мережі працюють протилежно. Додавання більшої кількості пристроїв зміцнює мережу з новими пристроями, якщо вони підключені до розетки, виконуючи функцію ретрансляторів.

Кожен пристрій у стандартній мережі WiFi повинен підключитися до маршрутизатора. Хоча пристрої в мережевих мережах зазвичай підключаються до центрального концентратора, вони також з'єднуються між собою. Ці пристрої не мають Wi-Fi. Взаємодія відбувається з концентратором за допомогою протоколу Z-Wave.

Сигнали можуть переходити з пристрою на пристрій - до 4 таких стрибків дозволено - тому можливе непряме контактування, що додає ще один рівень гнучкості в мережі.

Сітчасті мережі складаються з вузлів. Пристрої розумного дому, які використовуються у підключеному будинку, називаються вузлами при розгляді сітчастих мереж.

Повідомлення можна надсилати між вузлами, навіть якщо вони не знаходяться в прямому діапазоні. Ось де виклик перескоку надходить із сигналом, який проходить разом будь-якими засобами. Ця система дає вам розширене охоплення за рахунок невеликої та ледь помітної затримки у спілкуванні.

2.3.2 Z-WaveAlliance

Приватна технологія, що належить компанії Sigma, також має ліцензію на технологію Z-Wave та керує Z-WaveAlliance.

Цей альянс відповідає за сертифікацію та гарантує, що всі пристрої відповідають жорстким стандартам. Також потрібно, щоб кожен пристрій Z-Wave працював із кожним контролером Z-Wave.

Понад 600 виробників випускають понад 2400 пристроїв у рамках грандіозного Z-WaveAlliance.

2.3.3 ФінкціонуванняZ-Wave

Система Z-Wave функціонує на трьох шарах:

- Радіо
- Мережа
- Застосування

Пристрої Z-Wave поділяються на три широкі категорії:

- Датчики: керовані пристрої, що використовуються для комутації сигналів
- Контролери: метод управління для інших пристроїв Z-Wave
- Додатки: Звітні пристрої, що використовують як аналогові, так і цифрові сигнали для зв'язку

Є різні варіанти управління пристроями Z-Wave:

- Розумний телефон
- Планшет
- Комп'ютер
- Брелок
- Фізичний контроль

Незалежно від обраної форми управління, команда надсилається від контролера до концентратора. Команда здійснює маршрут до пристрою призначення.

Єдиний необхідний ввід користувача - це маніпулювання контролером.

Загальній мережі надається ідентифікатор мережі, а всі пристрої мають ідентифікатор вузла. Це гарантує, що у вас не буде конфлікту з сусідньою системою, а також, що всі дискретні пристрої також захищені.

2.3.4 Z-Wave: Основні характеристики

Архітектура сітки: є декілька пристроїв (вузлів), підключених до центрального концентратора. Керування пристроями Z-Wave відбувається у додатку на смартфоні за допомогою контролерів, настінного управління або голосових команд.

Mesh - мережа: За рахунок топології mesh - мереж Z-Wave є надійною. Усі сигнали направлені найефективнішим можливим шляхом. Якщо протокол не зможе знайти оптимальний маршрут, буде розгорнута альтернатива безпека: AES 128 є обов'язковим для будь-якого пристрою, який вимагає сертифікації Z-Wave, тобто безпека є залізною та порушення є дуже мало ймовірним.

2.4 Технологія BluetoothLowEnergy

BluetoothLowEnergy це інтелектуальна економічна версія безпроводової технології Bluetooth. Вона вже відіграє значну роль у перетворенні розумних гаджетів в ще більш розумні, роблячи їх компактними, доступними і менш складними.

BluetoothLowEnergy (BLE), також позиціонується як BluetoothSmart, починав свій розвиток як частина специфікації ядра Bluetooth версії 4.0. Спочатку, до прийняття групою BluetoothSpecialInterestGroup (SIG), вона була розроблена фірмою Nokia під назвою Wibree. Початковий акцент в ній робився на надання стандарту радіозв'язку з мінімально можливим енергоспоживанням, спеціально оптимізованого для отримання низької вартості, невеликої смуги пропускання, найнижчий рівень споживання електроенергії і невисокої складності. Ці цілі проекту очевидні з базової специфікації, яка демонструє прагнення зробити BLE справжнім стандартом з низьким енергоспоживанням, розробленим для практичної реалізації виробниками напівпровідникових компонентів і використання в практичних додатках при мінімальному споживанні енергії і мінімальному бюджеті. Це вже широко поширена технологія, реально здатна забезпечити тривалу роботу від однієї дискової батарейки. При тому, що технологія BLE чудова сама по собі, що зумовило феноменальну швидкість її поширення, це правильна технологія з розумними компромісами, яка з'явилася в потрібний час. За кількістю виробів, в яких вже міститься BLE, цей порівняно молодий стандарт набагато випереджає інші безпроводові технології в тій же точці їх життєвого циклу.

Проблемами, з якими зіткнувся класичний Bluetooth, є швидка витрата заряду батареї і часті втрати зв'язку, що вимагають періодичного повторного сполучення. Здатність успішно вирішити ці проблеми і стала однією з причин швидкого поширення BLE. Подальшому просуванню сприяв феноменальне зростання ринку смартфонів, планшетів і мобільних обчислень. Раннє і активне прийняття BLE важкоатлетами мобільної індустрії розгорнуло двері для більш широкого впровадження BLE. Це, в свою чергу, підштовхнуло виробників напівпровідників до

того, щоб сконцентрувати свої обмежені ресурси на тих технологіях, які, на їхню думку, швидше за все будуть розвиватися в довгостроковій перспективі.

У міру дорослішання ринків мобільних пристроїв і планшетів, потреба в з'єднанні цього обладнання з зовнішнім світом набуває величезний потенціал зростання. Це дає постачальникам периферійного обладнання унікальну можливість розробки інноваційних пристроїв, які вирішують проблеми споживачів, про існування яких сьогодні вони можуть навіть не підозрювати. Таким чином, в BLE поєдналося безліч переваг, які відкривають невеликим і моторним компаніям-розробникам доступ до потенційно величезного ринку з призначеними для вирішення конкретних завдань креативними та інноваційними продуктами при відносно скромному бюджеті проекту. Сьогодні BLE також дозволяє цим розробникам проектувати конкурентоспроможні продукти, що дозволяють спілкуватися з будь-якої сучасної мобільною платформою, використовуючи легко доступні мікросхеми, інструменти і стандарти.

2.4.1 Найнижче енергоспоживання

Все, від фізичної конструкції і до використовуваних моделей, підпорядковане мети підтримки мінімальної витрати енергії. Для зниження споживання енергії пристрій BLE більшу частину часу проводить в сплячому режимі. Коли відбувається якась подія, пристрій прокидається і передає коротке повідомлення на шлюз, персональний комп'ютер або смартфон. Максимальне / пікове споживання потужності становить менше 15 мА, а середнє - близько 1 мкА. У порівнянні з класичним Bluetooth, активна споживана потужність знижена в десять разів. У додатках з рідкісною періодичністю включення одна дискова батарея може забезпечити надійну роботу протягом 5-10 років.

2.4.2 Сумісність

Для сумісності з класичною технологією Bluetooth і невисокої ціни реалізації в невеликих пристроях з батарейним харчуванням існують два типи чіпсетів:

Дворежимні, з підтримкою функціональності як BLE, так і класичного Bluetooth;
Автономні BLE, оптимізовані для невеликих пристроїв з батарейним харчуванням, з акцентом на низьку вартість і малу споживану потужність.

У BLE використовується та ж технологія адаптивної стрибкоподібної перебудови частоти (AFH), що і в класичній Bluetooth. Це дозволяє BLE забезпечувати надійну передачу в умовах «зашумленого» ефіру типових для домашніх, промислових і медичних програм. Для мінімізації витрат і споживання енергії при використанні AFH кількість каналів в BLE скорочено до 40 при ширині кожного каналу 2 МГц, замість 79 каналів шириною 1 МГц, використовуваних в класичною технологією Bluetooth.

2.4.3 Співіснування безпроводових стандартів

Частоту 2.4 ГГц неліцензованому діапазону ISM використовують технології Bluetooth, безпроводові локальні мережі, IEEE 802.15.4 / ZigBee, а також кілька фірмових стандартів. При такій великій кількості технологій в одному радіопросторі завади можуть погіршити характеристики безпроводової мережі (тобто, збільшити затримки і зменшити пропускну здатність) внаслідок необхідності виправлення помилок і повторних передач. У відповідальних додатках вплив завад може бути знижено за рахунок частотного планування та спеціальної конструкції антени. Оскільки і в класичній Bluetooth, і в BLE використовується AFH, що мінімізує завади від інших стандартів радіозв'язку, обмін через Bluetooth стійкий і надійний.

2.4.4 Дальність зв'язку

Використовувана в BLE технологія модуляції дещо відрізняється від технології класичної Bluetooth. Ця різниця в модуляції забезпечує дальність зв'язку до 300 метрів при потужності передавача радіо-чіпсета 10 дБм (максимум, дозволений для BLE).

2.4.5 Простота використання та інтеграції

Зазвичай пікомережа BLE заснована на з'єднанні ведучого пристрою з декількома відомими. Пристрій може бути або провідним, або веденим, але не тим і іншим одночасно. Провідний пристрій вирішує, як часто ведені можуть виходити на зв'язок, а ведені можуть передавати дані тільки за запитом ведучого. Новою особливістю BLE, доданої до класичної Bluetooth, є функція оповіщення, за допомогою якої відомий пристрій може оголосити, що у нього є якась інформація для передачі ведучому. У сповіщенні може також міститися подія або результат вимірювання.

2.4.6 Технічні подробиці

BLE підтримує дуже короткі пакети даних (від 8 октетів мінімум до 27 октетів максимум), які передаються на швидкості 1 Мбіт / с. Всі з'єднання використовують вдосконалену технологію енергозбереження для максимального скорочення робочого циклу з метою мінімізації споживання енергії.

Для зниження завад від засобів радіозв'язку інших стандартів, що працюють в ISM діапазоні 2.4 ГГц, BLE використовує загальну для всіх версій Bluetooth технологію AFH. Переваги многотрактової маршрутизації збільшують енергетичний бюджет каналу зв'язку і ефективний робочий діапазон, а також оптимізують споживання енергії.

Значна частина інтелекту BLE реалізується контролером. Це дозволяє ведучому пристрою довше залишатися в стані сну і прокидатися по сигналу контролера тільки тоді, коли хост повинен виконати будь-яку дію. Відповідно, скорочується споживання струму, оскільки хост процесор, як правило, споживає більше енергії, ніж контролер BLE.

BLE може підтримувати швидке встановлення з'єднання і передачу даних за час всього 3 мс. Це дозволяє додатку всього за кілька мілісекунд встановити з'єднання і відправити аутентифіковані дані, а потім швидко розірвати з'єднання. Збільшення індексу модуляції дозволило забезпечити для BLE максимальну дальність зв'язку більше 100 метрів.

Для забезпечення максимальної завадостійкості BLE контролює всі пакети з допомогою надійного 24-бітного алгоритму CRC.

Високий рівень безпеки: повний алгоритм AES-128, який використовує блоковий протокол ССМ, забезпечує надійне шифрування і аутентифікацію пакетів даних, що гарантують безпеку інформаційного обміну.

BLE використовує 32-бітову адресу звернення на кожен пакет для кожного відомого пристрою, дозволяючи підключати мільярди пристроїв. Технологія оптимізована для з'єднань точка-точка, при цьому допускаються багатоточкові сполуки з використанням зіркоподібній топології.

2.5 Технологія Thread

Thread - це мережева технологія для побудови безпроводових меш-мереж з підтримкою IP-технології. Дана технологія дозволяє поєднувати пристрої в єдину інфраструктуру, яка має доступ в локальну / глобальну мережу. Через мережу LAN або інтернет користувач може управляти окремими вузлами, групами або ж цілою мережею.

Технологія Thread об'єднує в собі переваги мереж, що підтримують IP-протокол (таких як Wi-Fi) з можливістю беззавадного доступу до мережі інтернет або IP-мережі, і мереж з підтримкою ячеистої топології з можливістю

самовідновлення і ретрансляції повідомлень, а також підтримкою «сплячих» вузлів, які повинні житися від малої місткості.

Міжмережевий протокол (IP) це основний протокол зв'язку мережі Інтернет. Він надає основний механізм передачі datagram-повідомлень по IP-мереж, а також можливості по їх маршрутизації, що робить можливим міжмережеву взаємодію. Мережеві технології, які не підтримують міжмережевий протокол (IP), для роботи в IP-мережах повинні перетворювати повідомлення на спеціальному шлюзі, щоб мати можливість взаємодіяти з зовнішніми пристроями в IP-мережі. Цей процес має на увазі переупаковку даних з формату, прийнятого в конкретній мережі в IP-datagram-повідомлення. Це тягне за собою необхідність розшифровки переданого повідомлення на шлюзі і подальшого шифрування в IP-datagram-повідомлення.



Рисунок 2.2 – Маршрутизація пакетів в IP-мережу за відсутності підтримки IP-протоколу (ZigBee, BluetoothLE, ANT / ANT +)

З іншого боку, мережеві технології, такі як Thread і Wi-Fi, які мають вбудовану підтримку IP-протоколу, можуть передавати дані без додаткових накладних витрат.

Thread використовує фізичний рівень взаємодії (PHY) і рівень управління доступу до середовища (MAC), що відповідає стандарту IEEE 802.15.4-2006, що дає їм змогу працювати в частотному діапазоні 2,4 ГГц. Пропускна здатність каналу зв'язку становить 250 кбіт / с.

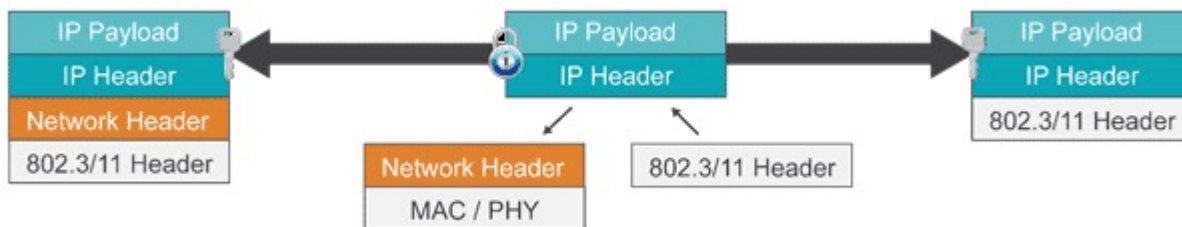


Рисунок 2.3 – Маршрутизація пакетів в IP-мережу при наявності підтримки IP-протоколу (Thread, Wi-Fi)

2.5.1 Топологія мережі Thread

У мережі Thread використовуються лише 2 типу пристроїв:

- Маршрутизатор (Router Eligible)
- Кінцевий вузол (End Device)

Маршрутизатор це вузол, який необхідний для підтримки ячеистої топології мережі (пошук маршруту, ретрансляція повідомлень і т.д.). Маршрутизатор, який організовує мережу буде автоматично призначений Лідером цієї мережі і крім стандартних завдань буде виконувати управління мережею:

- призначати вузли, які будуть брати участь в мережі в якості маршрутизатора
- видавати адреси для підключаються вузлів, використовую DHCPv6

Однак, вся інформація, що зберігається в лідерський вузлі дублюється в інших маршрутизаторах. Якщо виникли проблеми, інші маршрутизатори в мережі в автономному режимі можуть стати Лідерами, слідуючи правилу «одна мережа - один Лідер». Пристрої, які при підключенні до мережі вказали свій тип як Кінцевий вузол, не підтримують можливість здійснення будь-яких операцій, пов'язаних з маршрутизацією. Навпаки, вся зв'язок із зовнішнім світом здійснюється через «батьківські» вузли - маршрутизатори. При використанні змінних джерел живлення, кінцеві вузли можуть бути запрограмовані як «сплячі» для продовження терміну служби від одного комплекту. При втраті батьківського вузла і після декількох невдалих спроб відновити з ним зв'язок, кінцеві вузли в автономному режимі намагатимуться знайти нового «батька».

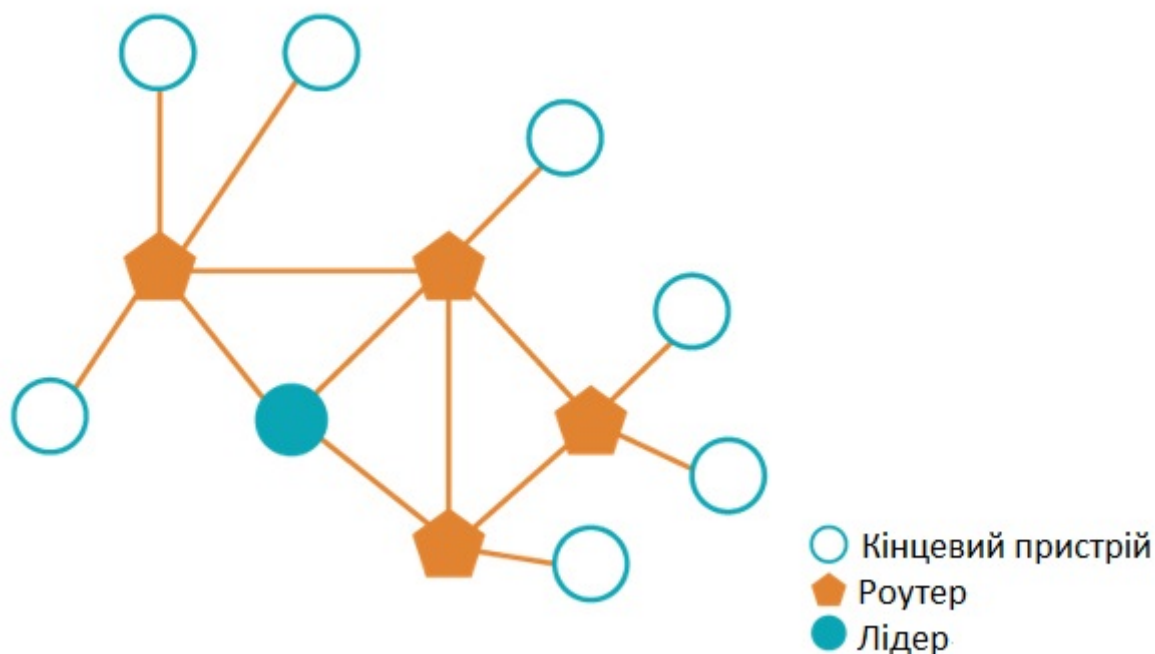


Рисунок 2.4 – Топологія Thread

2.5.2 Взаємодія з IP-мережами

Кожен пристрій в мережі Thread має власний IPv6-адреса, за допомогою якого воно може бути адресовано як всередині мережі (HomeAreaNetwork), так і з поза, використовуючи можливості Thread по маршрутизації IP-повідомлень. Для цих цілей використовуються спеціальні граничні роутери (Borderrouters, функціонально нагадують Wi-Fi-роутери), які дозволяють спілкуватися пристроїв Thread із зовнішнім світом через інтерфейси Wi-Fi, Ethernet і т.д. У одній мережі Thread може бути кілька таких роутерів.

Вузли в мережі Thread використовують префікси, отримані від граничного шлюзу (Borderrouter), для формування глобального IPv6-адреси або сформованого префікса для формування унікального локального адреси (ULA). Routing ID для вузла видається Лідером мережі. Для обміну повідомленнями в мережі Thread використовується протокол UDP. Спільно з UDP стек Thread використовує CoAP-протокол (Constrained Application Protocol), який дозволяє розширити можливості UDP. CoAP-протокол додає підтримку механізму повторних відправлень і визначає

порядок проходження повідомлень. Крім цього він додає підтримку HTTP-методів GET, POST, PUT і DELETE. Це дозволяє, при використанні зовнішнього CoAP-to-HTTP-проксі, працювати з пристроями Thread прямо з веб-браузера.

Висновки

У цій главі ми розглянули особливості безпроводових технологій. Розглянули топологію кожного протоколу а також їх технічні подробиці. Усі розглянуті технології схожі між собою. Кожна технологія має як ряд переваг так и недоліків, які ми розглянемо у третій главі.

3 ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ НА ОСНОВІ МОДЕЛІ OSI

3.1 Дослідження технології Wi-Fi

Розробка Wi-Fi заснована на базі стандартів безпроводових мереж IEEE 802.11x. Вони визначають лише тільки 1-й 2 рівень моделі OSI - матеріальний і канальний. Мережа Wi-Fi містить топологію "зірка", а це означає, власне що всі її вузли об'єднуються саме з центральною складовою - безпроводовим маршрутизатором. У подібній топології кінцеві прилади можливо додавати і видаляти з мережі, що не впливає на єдність її структури і передачу даних в ній.

Власне що стосується мережевого і транспортного значення, то для їх Wi-Fi як правило використовує інші нормальні протоколи - UDP або ж TCP для транспортного значення, і IPv4 або ж IPv6 для мережевого значення. А прикладний рівень, який, як ми вже знаємо, відповідає за сумісність приладів, не визначений рішуче, і цілком відданий на відкуп виробникам програмних і апаратних висновків.

3.1.1 Переваги Wi-Fi як протоколу домашньої автоматизації

Wi-Fi - це сильне і надійне безпроводове з'єднання, яке благополучно застосовується для зведення локальних сіток вже багато років. 802.11 став масовим стандартом зв'язку, тому що пропонує велику кількість гнучких функцій і кожен день поліпшується Інститутом інженерів електротехніки та електроніки (IEEE).

Створений для швидкого обміну важливими розмірами даних на коротких відстанях, Wi-Fi дуже добре справляється зі своїм завданням. Головні характеристики, такі як спектр покриття або ж швидкість передачі даних, відрізняються між різними варіаціями еталона 802.11. Але в більшості випадків простого побутового безпроводового маршрутизатора досить, щоб гарантувати покриття мережі для маленької житлоплощі. У величезних будівлях можна

збільшити чисельність точок доступу або ж ретрансляторів сигналу для збільшення покриття.

Wi-Fi має можливість просто транслювати відеопотоки високої чіткості, а межа пропускної можливості набагато вище, ніж необхідність середнього користувача. Деякі більш старі версії еталона 802.11 мають лімітування 11 Мбіт / с або ж 54 Мбіт / с, але широко застосовується в даний момент 802.11n здатний транслювати вже десятки і сотні Мбіт в секунду, а більш свіжий 802.11ac - ще більше. Ці цифри, абсолютно, виглядають дуже добре на тлі інших відомих висновків для господарської автоматизації. Міра їх пропускної можливості виражається в Кбіт / с, а не в Мбіт / с.

Крім того, одна з ключових переваг Wi-Fi - повсюдна доступність інфраструктури 802.11. Даний стандарт вбудовується в нові ноутбуки, телефони та планшети, містить величезний сенс з точки зору реалізації керуючих додатків розумного житла і "інтернету речей".

3.1.2 Недоліки Wi-Fi як протоколу домашньої автоматизації

Перераховані вище видатні якості загальновідомі. Завдяки їм Wi-Fi і стала буденною технологією безпроводового доступу в Онлайн. Але коли мова заходить про домашню автоматизацію, висока швидкість доступу в Онлайн та ймовірність швидко транслювати великі розміри інформації - це не ті характеристики, на які ви будете звертати хоч якусь увагу. Більше того, здатності Wi-Fi в даному проекті ек підходять для переважної більшості розумних програмних стандартів автоматизації житла. Ці стандарти працюють в середовищі, де звичайні прилади передають звичайні керуючі команди (такі як "включити / вимкнути"), сигнали зміни стану або ж найменші розміри даних (наприклад, підсумки вимірювань, що передаються датчиком). Найвище енергоспоживання WI-FI не дозволяє робити належно приладу розумного будинку.

Wi-Fi містить дуже невисоку енергоефективність, щоб застосувати її в автономних датчиках розумного будинку. Сама по собі пропускна спроможність - не проблема, але її допомога пов'язана зі важливим енергоспоживанням. Будучи швидкісним стандартом безпроводового зв'язку, Wi-Fi надмірно енерговитратна для "Інтернету речей". Безперечно, власне, що енергоспоживання не грає величезної ролі, в разі якщо будь-який прилад підключено до постійного джерела живлення - звичайної електричної розетки, патрону лампи і т.п. Але це робить великим завданням для тих приладів, які повинні працювати від автономних джерел живлення без проводів. Наприклад, самостійний датчик переміщення, задимлення, відкриття / закриття дверей на базі Wi-Fi робити не має сенсу: його акумулятор швидко розрядиться. Іншими словами, не звертаючи уваги на широку поширеність і значну швидкість передачі даних, Wi-Fi елементарно не має можливість дієво підтримувати найважливіші компоненти розумних осель - незалежні безпроводові детектори і виконавчі прилади. А без них домашняавтоматизація втрачає практичне значення.

Ще одне значне лімітування з'являється через топології Wi-Fi-мережі. Залежність всього трафіку від центрального маршрутизатора містить неабиякий дефект: як тільки-но маршрутизатор виходить з ладу, окремі вузли мережі припиняють взаємодіяти один з одним. А це веде до збою всієї мережі автоматизації. Природньо, можна очікувати, що величезну частину часу маршрутизатор Wi-Fi буде працювати розмірено. Нерідко дійсно і трапляється. Але як тільки-но він "зависає" або ж ламається, негайно ж з'являються великі труднощі: цілий розумний жбудинок закінчить працювати. Не варто ще забувати про те, що при підміні вийшовшого з ладу безпроводового маршрутизатора, швидше за все, знадобиться перебудова і конфігурація мережі з нульової позначки.

Wi-Fi можна знайти в будь-якому новому телефоні або ж ноутбучі. В тім разі даний потенціал неможливо втілити в життя цілком. Не звертаючи уваги на те, власне, що телефон і прилад розумного житла за допомогою Wi-Fi використовують одну і ту ж "мову спілкування", дана асоціація не рахується прямою. Вона щоразу виконується крізь центральну точку доступу до мережі. Ось чому прилади Wi-Fi не

можуть застосувати деякі значущі функції, такі як, наприклад, виявлення приладів, що знаходяться поблизу.

Беручи до уваги, що буквально будь-яка людина має телефон за підтримкою Wi-Fi, можна припустити, власне, що додавання нових розумних приладів в Wi-Fi-мережу буде легкою справою. На жаль, це не так. Перш ніж додати прилад розумного житла в Wi-Fi-мережу, треба заявити йому пароль мережі. Це просто влаштувати, в разі якщо ви бажаєте включити ноутбук або ж телефон. Але завдання ускладнюється, в разі якщо на вашому приладі немає ні клавіатури, ні екрану. Чи можливо доручити цю роботу телефону, так як він ще "говорить" мовою Wi-Fi? Чому б не застосувати його, щоб заявити пристрою пароль? Задовільна думка, але проблема в тому, власне що для цього ваш розумний прилад на початку треба підключити до мережі. А це повертає нас туди, звідки ми почали. У більшості випадків для додавання розумних приладів в мережу Wi-Fi треба ввести особливий мобільний додаток або ж десктопну утиліту, слідом за тим перемістити будь-яке додавання приладу в режим сполучення, встановити скрізь пароль Wi-Fi, а вже слідом за тим - додати прилад в систему домашньої автоматизації. Деякі постачальники зайшли далеко, що додали у власні розумні Wi-Fi-пристрої порти microUSB саме для цілей початкового включення і опції. Але це не вирішує проблему з додаванням, напевно чи вам сподобається застосувати USB-порти для додавання в мережу розумні детектори диму або ж переміщення, поставлені в недоступних місцях.

Таким чином, Wi-Fi практично ніколи не слід розглядати як фундамент розумного будинку. Виняток - ті рідкісні випадки, коли потрібно тільки надійне з'єднання з хмарою, і ви не плануєте впроваджувати розумні пристрої на основі інших стандартів.

Таблиця 3.1– Переваги та недоліки Wi-Fi ка протоколу домашньої автоматизації

Переваги	Недоліки
Широко поширений в комп'ютерах і мобільних пристроях	Високе енергоспоживання не дозволяє використовувати Wi-Fi в автономних датчиках і актуаторах розумного будинку
Забезпечує високу швидкість передачі даних	Мережева топологія "зірка" не гарантує відмовостійкості мережі
Має достатній радіус дії	Сумісність пристроїв різних виробників під питанням, оскільки прикладний рівень OSI не стандартизований
	Складний процес додавання в мережу деяких пристроїв
	Проблеми з безпекою, такі як механізм управління ключами

3.2 Z-Wave згідно моделі OSI

Z-Wave охоплює всі рівні моделі OSI, від фізичного до прикладного. Це гарантує піднесений рівень сумісності обладнання для домашньої автоматизації від різних постачальників. Z-Wave - добре налагоджений протокол, спрямований на обмін короткими командами і повідомленнями між приладами, власне що призводить до мінімальної кількості завантаженості радіоканалу і знижує можливість втрати даних.

Z-Wave користується топологією мережі (mesh-мережі). Протокол розроблений таким чином, власне, що вузли мережі, що виробляють роль ретрансляторів, мають можливість перенаправляти крізь себе зсигнал, доки не дістанеться адресата. Подібнерішення не лише тільки дозволяє розширити радіус дії

безпроводової мережі, але і збільшує її надійність. У разі переміщення / деактивації / виходу з ладу будь-якого вузла, мережа не стане паралізована, а продовжить роботу в штатному режимі: повідомлення почнуть механічно направлятися крізь ретранслюючі вузли мережі в обхід вийшовшого з ладу.

Будь-яка закономірна мережа Z-Wave має можливість підтримувати роботу до 232 приладів. При потребі включення найбільшої чисельності приладів застосовується об'єднання сіток. Деяка кількість сіток Z-Wave можуть безтурботно уживатися в одній системі, не заважаючи один одному. Це досягається мінімізацією обсягу переданого пакета і обов'язковою вимогою до малого навантаження на радіоканал, яке зобов'язує прилад перебувати в стані передачі максимум 1% часу. Втім вузли різних сіток не мають можливості "бачити" один одного і, відповідно до цього, будь-яким чином зв'язуватися один з одним. Зв'язок між мережами виповнюється крізь прилади, що виконують роль мережових мостів.

Прилади в одній мережі можуть обмінюватися інформацією між собою, в тому числі і коли знаходяться за межами зони прямої видимості. В даному випадку прилад користується проміжними вузлами (інші прилади в цій же мережі, не рахуючи тих, які живляться від батарейок і величезну частину часу працюють в «сплячому» режимі через економію заряду батареї), щоб передати інформацію іншим пристроєм, коли вони розташовуються за межами радіусу дії першого приладу.

У будь-якої мережі Z-Wave є провідний контролер (з нього, саме, і настає зведення мережі), на який покладено прямі обов'язки додавання нових конструкцій в мережу і видалення давніх, складання карт маршрутизації, забезпечення безпечного включення, здатності робити сценарії автоматизації та інших функцій з організації та контролю роботи мережі. У мережі є можливість знаходитися одному або ж кільком вторинним контролерам, які для нормальної роботи подають запит на інформацію про топології мережі у головного контролера. Як правило головним контролером вважається той, з якого стартувало зведення мережі. Часто нові прилади Z-Wave можна додати в мережу з підтримкою QR-коду або ж пін-коду. Дана безпечна процедура трапляється один раз під час установки нового приладу, після чого прилад є власністю даної мережі.

Особливою рисою екосистеми Z-Wave на початку було те, власне, що вона навмисно розвивалася як замкнутий пропріетарний протокол, захищений численними патентами керуючої компанії (спочатку - Zensys, слідом за тим - Sigma Designs, нині - Silicon Labs). Всі функції протоколу продані в програмному коді компанії-власниці технології і поставляються виробникам оснащення в скомпільованому вигляді згодом підписання ліцензійного договору.

З одного боку, закритість технології - це мінус, наприклад як без пізнання пропріетарних специфікацій сторонні розробники не мають можливості на власний розсуд застосувати протокол для розробки програмного забезпечення для управління приладами Z-Wave. Це ускладнило вторгнення Z-Wave на ринок. Втім володарі розумних будинків від подібної «закритості» виявилися у великому виграші. Бренд Z-Wave - єдиний на ринку домашньої автоматизації, який має можливість забезпечувати взаємосумісність застосовуваних приладів автономно від виробника, вартості, активних завдань, поколінь мікросхем, визначеного приладу і т. д.

Нижні рівні (фізичний і каналний) протоколу Z-Wave стали розкритими ще в 2012 році і з тих часів описуються стандартом Інтернаціонального Міжнародного союзу електрозв'язку ITU-T G.9959. Вони відповідають саме за безпроводову передачу даних, чітко описуючи застосування частоти, методи кодування і адресації.

У 2016 році Sigma Designs виклала в відкритий доступ офіційну специфікацію протоколу Z-Wave. Зокрема, були розміщені класи команд (описують, як складається кожна окрема команда і як інтерпретувати згортки даних) і класи приладів (описують специфікацію існуючих приладів, і те, як ці прилади, в залежності від власного типу, сприймають різні команди). Було розміщено опис найсвіжіших специфікацій шифрування в Z-Wave, що отримали назву Security 2 (S2). Крім того, оприлюднено опис Z / IP (Z-Wave over IP) - програмної надбудови для передачі пакетів Z-Wave поверх TCP / IP. Це важливо спростило розробку сторонніх веб-додатків для Z-Wave.

Все ще залишаються замкнутими мережевий і транспортний рівні, які забезпечують безпрецедентну для гілки міцність роботи величезних Z-Wave-

будинкових мереж та відповідають за маршрутизацію повідомлень в мережі розумного будинку, їх ретрансляцію і свідоцтво отримання.

3.2.1 Переваги Z-Wave

Творці Z-Wave на багато років перевершили свій час, і Mesh-мережа тривалий час володіла оригінальним функціоналом, що дає даному протоколу помітну конкурентну перевагу. В даний момент мови про наявність mesh-топології лише тільки у Z-Wave вже не йде. Але власну актуальність сітчасті мережі не втратили, залишаючись до цього найкращим рішенням для домашньої автоматизації. На відміну від безлічі суперників, Z-Wave є вже багато років, і творці до гідності відшліфували процес маршрутизації повідомлень. З усіх представлених на ринку домашньої автоматизації, приладуи Z-Wave вважаються, напевно, найбільш енергоефективними, надійними, безпечними і економічними з точки зору часу ефіру, займаного під обмін даними.

Щоб нівелювати затримки при передачі і не перевантажувати мережу, допускається використання до 4 проміжних вузлів для транзитної передачі даних. З урахуванням такого, що радіус дії в зоні прямої видимості передових модулів Z-Wave оформляє близько 40 метрів (а нове покоління приладів Z-Wave на чіпсетах 700-й серії збільшує до 100 м), то підсумкової дальності передачі сигналу в одній мережі Z-Wave цілком достатньо для реалізації більшості великих планів домашньої автоматизації.

Великим оригінальним плюсом технології Z-Wave вважається ймовірність буквально моментального самолікування мережі, коли якийсь вузол перестає відповідати. Вона досягається завдяки використанню процедури Explorer Frame («Дослідницький кадр»), яка запускається автоматично. Для визначення всіх можливих «робочих» маршрутів і, відповідно до цього, відновлення працездатності мережі Z-Wave буде потрібно не більше секунди. При цьому з виходом у світ процедури Explorer Frame в мережі Z-Wave стало цілком ймовірно повноцінно

застосувати переносні прилади, функціональність яких в більш давніх реалізаціях була міцно обмежена.

Ще 1 функція, що підвищує відмовостійкість і швидкодію мережі Z-Wave, - асоціації між приладами. Завдяки даній функції, прилад має можливість відправляти команду розташованому поблизу іншому пристрою, минаючи центральний контролер. Наприклад сирена має можливість підключитися по датчику переміщення швидко, не чекаючи, поки ж їй прийде команда від контролера. Виконавши впроцедуру, прилад вишле контролеру доповідь про виконання. Це не лише тільки прискорює спрацювання виконавчих приладів, але і збільшує надійність серйозних вузлів мережі. Наприклад, зв'язка "датчик-виконавчий пристрій" буде працювати, в тому числі і в разі якщо контролер вийшов з ладу. Так, користувач перестане отримувати від контролера сповіщення про спрацювання приладів. Але завдяки асоціаціям самі ці прилади продовжать працювати в зв'язці. Для цього вони повинні бути знаходяться поблизу один від одного, тобто для проходження команди не знадобиться маршрутизація. Крім того, вони зобов'язані мати на увазі ймовірність спільної роботи (наприклад датчик протікання і автоматичний кульовий кран).

Ще одна перевага Z-Wave - захищеність. Тут вона подана на найвищому рівні. Розробка Z-Wave використовує ті ж технології шифрування, власне що і системи онлайн-банкінгу. Свіжий стандарт захищеності, знайомий як Security 2 (або S2), став обов'язковим для сертифікації всіх розумних приладів Z-Wave згодом 2 квітня 2017 року. Він покращує стандарти шифрування для змоги реалізації обміну даними між вузлами, а ще задає нові процедури включення нових приладів до мережі розумного житла з підтримкою оригінальних для всякого приладу PIN-кодів або ж QR-кодів. Новий ступінь оборони аутентифікації ручається, власне що хакерам не вийде взяти під контроль прилади під час включення їх до мережі. S2 вважається найбільш прогресивною системою захищеності, доступною на ринку домашньої автоматизації. Творці Z-Wave приділили удосконаленню оборони, Z-Wave за останні пару років значимо зміцнив позиції на ринку мудрих систем захищеності,

ставши, наприклад, абсолютним фаворитом для такого показового розділу, як розумні дверні замки.

Z-Wave працює в неліцензованому частотному діапазоні 800-900 МГц, виділеним для приладів дрібного радіусу дії. Особлива лінія даних частот - дієздатність впевнено долати всілякі завади, в тому ж числі великої кількості перекриттів і стінок. Це є першопричиною для переваги на ринку домашньої автоматизації і Z-Wave приладів (при цьому вони ще й енергоефективні). Для даного частотного діапазону ще властива невелика кількість завад, які виконуються іншими приладами, що діють на цих же частотах. З урахуванням того, що інші протоколи, які створюють конкуренцію технології домашньої автоматизації зобов'язані знаходитися в надзавантаженому діапазоні 2,4 ГГц, який використовує велику чисельність приладів по всьому світу, в тому числі і ці далекі від безпроводового зв'язку, як звичайні мікрохвильові печі, практично недоступні в робочому діапазоні Z-Wave (і як наслідок - малий час затримки), робиться ще одним конкурентоспроможним плюсом цього протоколу домашньої автоматизації.

На сьогоднішній день на ринку представлено більше 2400 сертифікованих (сумісних один з одним) назв приладів від більше ніж 700 фірм. Більше 100 млн розумних Z-Wave-пристроїв вже працюють в мільйонах домівок по всьому світу. Це вражаюче вторгнення на ринок, напевно, вважається досить міцною заявкою в гонці за переважання на IoT-ринку між протоколів безпроводового зв'язку. Великий асортимент приладів Z-Wave вигідний користувачам: з Z-Wave вони можуть обирати все, власне що завгодно: перелік можливостей, дизайн, вартість і в тому числі і колір продукту. При цьому вигоди від цієї свободи вибору не обмежені з точки зору сумісності приладів від різних постачальників. Гігантську роль в питанні сумісності відіграє сертифікаційна програма, розроблена галузевим консорціумом Z-Wave Alliance. Випробування, проведені альянсом, ручається, власне що всілякі сертифіковані прилади, автономно від їх виробника, стануть чудово ладнати між собою. Цим чином, гарантована сумісність вважається найсильнішим конкурентоспроможним плюсом Z-Wave. І це при тому, що протокол ще гарантує

зворотну сумісність з усіма попередніми версіями, власне що вважається ще однією оригінальною особливістю для IoT-ринку.

3.2.2 Недоліки Z-Wave

У Z-Wave залишилося не така велика кількість слабких місць: за роки існування технології її встигли дуже добре налагодити. Напевно, саме з дефектів виливаються і плюси: це частотний діапазон. Вибір низькочастотного, розміреного і більш вільного діапазону для приладів дрібного радіусу дії, а не більше відомого і завантаженого (2,4 ГГц) виявився далекозорим і вірним рішенням, що врятувало користувачів розумного будинку Z-Wave від серйозних завдань з завадами в міцно завантажених «частотах Wi-Fi». Але у всього є своя ціна. Історично склалося, власне що в різних державах для роботи приладів дрібного впливу виділені різні частоти. Наприклад, для всієї Європи (країни CEPT), а ще Китаю і ряду інших держав Азії - це 868,42 МГц. А ось в USA і Мексиці ці частоти зайняті технологією GSM, в наслідок цього рішення Z-Wave там працюють на частоті 908,42 МГц. Російська Федерація, яка поставила свій підпис в договір CEPT, але наприклад його і не ратифікувала, пішла своїм шляхом і обрала для Z-Wave діапазон 869,0 МГц. Власне що це означає з точки зору простого користувача? Докупувати свіжий продукт в іншій країні і включати його до власної мережі домашньої автоматизації треба з величезною пересторогою. Наприклад прилад, зроблений для ринку США, стане несумісний з приладами "російського" спектра.

Крім того, як ми вже зауважували раніше, тривалий час Z-Wave розвивалася як замкнута розробка. Це дозволило творцям забезпечувати чудову сумісність, захищеність, відмовостійкість і т. Д. Але ця «закритість» обходиться дорожче в розробці приладів. В наслідок цього висновку Z-Wave можна назвати не найбільш економним варіантом для розумного житла. Інша справа, питання ціна / якість, де розробка Z-Wave не залишила суперникам буквально практично ніяких шансів.

Таблиця 3.2 – Переваги та недоліки протоколу Z-Wave

Переваги	Недоліки
Світовий лідер за поширеністю і кількості інсталюваних пристроїв в системах розумного будинку	У різних країнах для Z-Wave використовуються різні радіодіапазони, на що необхідно звертати увагу при покупці в інтернет-магазинах
Висока відмовостійкість і масштабованість завдяки комірчастій топології мережі, а також механізмам самовідновлення і асоціацій	
Високий рівень безпеки, реалізований набором протоколів S2	
Низький рівень споживання енергії пристроїв	
Відмінна взаємна сумісність пристроїв Z-Wave різних виробників завдяки сертифікації, виконуваної консорціумом Z-Wave Alliance	
Захищеність від впливу інших пристроїв Wi-Fi, Bluetooth, мікрохвильовими печами та іншим обладнанням, що працює в діапазоні 2,4 ГГц	

3.3 ZigBee в рамках моделі OSI

Комплект протоколів ZigBee визначає лише тільки верхні значення моделі OSI - мережевий, транспортний і прикладний. Він споруджений поверх еталона IEEE 802.15.4, який визначає нижні значення безпроводової мережі, спрямованої на

кінцеві прилади (а не на користувачів, як, наприклад, Wi-Fi), і характеризується невисоким енергоспоживанням і невисокою швидкістю передачі даних. Стандарт IEEE 802.15.4 підтримується декількома постачальниками чіпів і застосовується не лише тільки для ZigBee, але і у декількох десятках інших протоколів. В якості робочого спектра даний стандарт визначає неліцензовані частоти 2,4 ГГц (по всьому світу), 915 МГц (для Америки і Австралії) і 868 МГц (для Європи). Гранична швидкість передачі даних досягає 250 Кбіт / с в діапазоні 2,4 ГГц, 40 Кбіт / с в діапазоні 915 МГц і всього 20 Кбіт / с в діапазоні 868 МГц. В наслідок цього буквально всі прилади ZigBee працюють лише тільки на частоті 2,4 ГГц.

На відміну від Z-Wave, яка для доставки пакетів до окремих вузлів мережі користується схемою маршрутизації від джерела повідомлення, ZigBee користується маршрутизацією від адресата. Цим чином, в реалізації mesh-мережі ZigBee бере участь три класи приладів: координатор ("мозок" мережі, який її створює і координує її роботу), маршрутизатор (постійно діяльний, в наслідок цього повинен бути підключений до джерела постійного струму; відповідальний за підключення і сервіс до 32 кінцевих приладів, в наслідок цього їх розташування потребує оптимізації, а чисельність належить бути необхідним для сервісу всіх приладів в мережі; ще вважається головною складовою при трансляції та динамічної маршрутизації пакетів в мережі) і кінцеві прилади (більшу частину часу присутні в сплячому режимі через економію заряду батареї, можуть брати на себе і відправляти пакети, але не беруть участь в їх ретрансляції). Таким чином, ZigBee пропонує досить чудовий з технічної точки зору підхід до організації mesh-мережі, але він, як і в випадку з Z-Wave, здатний гарантувати самовідновлення мережі і має можливість швидко перенаправити пакети даних, щоб гарантувати їх доставку, в разі якщо який-небудь вузол не працює або ж не відповідає.

3.3.1 Переваги ZigBee

ZigBee - зріла розробка домашньої автоматизації. На даний момент Zigbee

Alliance налічує сотні користувачів, а на ринку є тисячі всіляких рішень із підтримкою Zigbee. Величезне ринкове вторгнення, абсолютно, вважається міцною стороною технології, коли у користувачів є можливість вибору.

ZigBee -Відкритий стандарт безпроводового зв'язку, що перш за все виглядає привабливим з точки зору творців і виробників. Це дозволяє їм бути більш гнучкими у виборі важливої їм функціональності, а ще з найменшими витратами виводити на ринок нові продукти. Так, наприклад, завдяки цьому ZigBee мав непоганий тріумф на корпоративному ринку. Зокрема, деякі кабельні ТВ-мережі і телекомунікаційні фірми скористалися ZigBee в власних сет-топ-боксах і супутникових трансиверах, а комунальні фірми додавали за допомогою цього протоколу розумні лічильники електрики і води, щоб удосконалити якість прогнозу, контролю та управління вживання пропозицій для своїх користувачів.

Провідний козир Zigbee - орієнтація на економних покупців. Даному у багато чому сприяє не тільки лише відкритість еталона, але і простий розклад Zigbee Alliance до сертифікації нових товарів, що дозволяє виробникам застосувати у власних рішеннях лише тільки ту конфігурацію, яка їм важлива. Таким чином, мережа Zigbee - економний варіант реалізації безпроводової домашньої автоматизації.

Як ми вже зауважували, енергоспоживання можна віднести до міцної сторони рішень за допомогою Zigbee. Не звертаючи уваги на те, власне, що заслуги Zigbee в даному аспекті не так значні, як у провідних суперників (Z-Wave і в тому числі і Bluetooth), окремі прилади Zigbee готові відпрацювати до 2 років без потреби підміни батареї. В цілому, це задовільнило показник для передового ринку домашньої автоматизації.

ZigBee володіє непоганою масштабованістю. Наділена підтримувати до 65 000 вузлів, даний стандарт на теоретичному рівні має можливість гарантувати велике охоплення, не звертаючи уваги на порівняно маленький радіус дії окремих модулів (10-20 м в приміщенні). Правда, до даних показників слід ставитися з долею скепсису. Наприклад, мережі з чотиризначною кількістю вузлів стикаються з неабиякими завданнями при підтримці безперебійної роботи в тому числі і в

лабораторних умовах. Затримки в обміні даними, як правило, відбуваються в тому числі і в разі значно менших розгортань (сума яких обчислюється лише кількома сотнями пристроїв). І це не дивно, беручи до уваги що прецедент, власне що ZigBee працює в надзавантаженому діапазоні 2,4 МГц, а максимальна швидкість передачі даних досягає 250 Кбіт / с.

3.3.2 Недоліки ZigBee

ZigBee погано справляється з ситуаціями, коли в зоні впливу мережі є міцні завади, що формуються іншими приладами. Будучи одноканальним рішенням, ZigBee далеко не всякий раз має можливість дієво боротися з завадами, які часто зустрічаються в перевантаженій смузі 2,4 ГГц, порд з застосовуваними протоколами з такими технологіями, як Wi-Fi або ж Bluetooth. І в найближчому майбутньому ситуація буде ще гірше, наприклад як завантаженість смуги 2,4 ГГц з кожним роком буде зростати. Труднощі для ZigBee погіршує ще те, що стандарт IEEE 802.15.4, що визначає матеріальний рівень стека протоколів ZigBee, що обмежує швидкість передачі даних до 250 Кбіт / с, знаходиться під контролем IEEE. Він застосовується не лише тільки ZigBee, але і десятками іншими рішеннями. В наслідок цього, щоб, в разі потреби внести в нього будь-які конфігурації, що відповідають потребами ринку, ZigBee Alliance буде необхідно вступити в тривалі переговори з IEEE. Результати цих переговорів непередбачувані, наприклад як IEEE переслідує особисті цілі. В наслідок цього ці організації, як Z-Wave Alliance, цілком контролюють власні протоколи, присутні в значно більш вигідному становищі. Z-Wave Alliance визначає будь-який окремий рівень моделі OSI, і в наслідок цього всі рішення, що стосуються будь-якого аспекту зв'язку, присутні в руках однієї організації.

Власне що стосується захищеності, то ZigBee пропонує розмашистий діапазон розширених заходів для забезпечення необхідної оборони даних, якими обмінюються розумні пристрої. З 128-бітовим алгоритмом AES, застосовуваним для

шифрування даних і аутентифікації, і 3-ма типами ключів, що застосовуються для управління захищеністю, кінцевим користувачам на перший погляд не варто хвилюватися. Втім, час від часу з'являються неспокійні анонси про проблеми захищеності, виявлених в пристроях за допомогою ZigBee. Наприклад, в середині 2015 року компанія Cognosec показала на конференції Black Hat USA, як можливо застосувати деякі уразливості в продуктах ZigBee. Вони, в провідному торкалися беззахисного формування парних ключів при включенні нового приладу до мережі. У заяві, розміщеній ZigBee Alliance, організація показала, власне що метод злому, описаний в доповіді Cognosec, їй популярний і може бути застосований до будь-якої системи ZigBee, що використовує обмін відкритими ключами при додаванні до мережі. В чому ж проблема, чому дана уразливість все ще є, якщо вона популярна на протязі довгострокового часу? Все прозаїчно елементарно. Основна маса завдань захищеності з мережами ZigBee не мають ніякого відношення до самого протоколу. Не звертаючи уваги на ймовірність застосування конкретних вразливостей, в тому числі і Cognosec приймає в своїй доповіді, власне що функції, які надаються стандартом ZigBee, можуть бути досить просунутими і надійними. Проблема в тому, власне, що виробники не повинні вводити їх у власні продукти цілком. ZigBee Alliance не вимагає, щоб виробники приладів трималися всієї специфікації. Натомість цього їм надається воля вибору тих пристроїв, які важливі для певних рішень. У підсумку, бажаючи зекономити, виробники нерідко використовують лише тільки найменший набір функцій захищеності, важливий для проходження процедури сертифікації. І ці «обрізання» реалізації як правило призводять до уразливості всій мережі.

В цілому, не звертаючи уваги на перераховані вище дефекти, ZigBee, абсолютно дієва розробка. За ідеєю, вона зобов'язана чудово ладити із більшою частиною завдань домашньої автоматизації. Все було б як раз так, в разі якби не одне «але». Дуже часто, прилади ZigBee різних виробників несумісні один з одним. Як це взагалі можливо для настільки зрілої технології, з мільйонами працюючими рішеннями по всьому світу, і яка претендує на лідерство на IoT-ринку? Всьому виною дуже м'яка політика діючої сертифікації, закликає повернути як можливо

більше виробників додавати технологію ZigBee у власні прилади. Щоб полегшити для виробників впровадження ZigBee у власні продукти і закласти базу для сумісності між різними висновками від різних вендорів, ZigBee Alliance зробив ряд стандартизованих специфікацій (профілів) на прикладному рівні, таких як профіль Home Automation, профіль Remote Control або ж профіль Light Link. Кожен з них буквально патерни зв'язку між мудрими приладами, що входять в ту чи ж іншу категорію товарів.

Програма сертифікації ZigBee Alliance перевіряє, чи відповідає цей продукт відповідному, гарантуючи, що прилади, які мають один і той самий ж профіль, повинні спілкуватися один з одним, в тому числі і в разі якщо виготовлені різними постачальниками. Але в питанні застосування пристроями захищеності, виробникам приладів надана гігантська воля вибору. Вони самі вирішують, які з даних профілів стануть застосувати у власних продуктах. Великі виробники негайно користувалися даною свободою, створивши особисті пропрієтарні рішення.

Коли мова йде про великі бренди, доходить до такого, власне, що в разі якщо ви виберете з магазинної полиці 2 випадкових прилади ZigBee різних виробників, то, швидше за все, вони не зможуть "спілкуватися" один з одним безпосередньо. Великі фірми найчастіше роблять пропрієтарні ZigBee-рішення, здатні перекидатися даними лише тільки з іншими приладами під одним і тим же брендом. Є цільні відокремлені екосистеми ZigBee різних брендів: Xiaomi, Philips Hue, IKEA. Поєднати контролери 1-го бренду з датчиками і виконавчими приладами іншого просто "з коробки" не вийде. Наприклад, щоб контролер розумного будинку Xiaomi мав можливість керувати лампами Philips Hue, буде необхідно купувати ще контролер Philips. Контролери стануть контактувати між собою (але не з кінцевими приладами іншого бренду) крізь програмні інтерфейси додатків на базі IP.

Роблячи ставку на ZigBee як на базу автоматизації вашого розумного житла, для вас буде необхідно автономно перевіряти на сумісність все підібрані вами приладами різних брендів. Постраждала крах сертифікаційна програма консорціуму ZigBee Alliance, на жаль, практично ніяких стандартів сумісності надати не може.

Якраз в поганій сумісності прихований дефект ZigBee. І він об'єднує нанівець основну масу переваг даної технології.

Таблиця 3.3 – Переваги та недоліки ZigBee

Переваги	Недоліки
Зріла і поширена технологія	Використовує діапазон 2,4 ГГц, де сильні завади від Wi-Fi, Bluetooth, мікрохвильових печей і т.п.
Висока відмовостійкість і масштабованість завдяки комірчастій топології мережі	Вкрай погана сумісність між пристроями ZigBee різних виробників через занадто м'яких умов сертифікації, висунутих консорціумом ZigBee Alliance
Низький рівень споживання енергії	Проблеми з безпекою через недотримання виробниками вимог сертифікації

3.4 Протокол Thread в моделі OSI

Thread працює поверх вже згадуваного нами раніше еталона радіозв'язку IEEE 802.15.4, який вважається фундаментом мережі ZigBee. Сам же протокол Thread визначає лише тільки мережевий і транспортний рівні моделі OSI, призначені для укладання таких завдань, як маршрутизація, розгортання і забезпечування захищеності. Thread не охоплює прикладний рівень. Власне що це означає з точки зору практичного застосування?

Грунтуючись на фізичній інфраструктурі 802.15.4, Thread увібрав в себе всі її міцні і слабкі сторони, про яких ми згадували при розгляді протокола ZigBee. Це невисока ціна зв'язку з найближчими приладами, невисокий ступінь споживаної енергії, одно канальне рішення з найбільшою швидкістю передачі даних 250 Кбіт / с,

а ще крайня завантаженість робочого діапазону 2,4 ГГц, тим більше в міських умовах.

3.4.1 Переваги протоколу розумного будинку Thread

Слід зазначити, що залежність Thread від стандарту 802.15.4 не така сильна, як у випадку ZigBee. На додаток до 802.15.4, Thread гарантує самовідновлювання, засноване на IP, безпечне mesh-рішення, яке дозволяє кінцевим користувачам просто додавати власні прилади до інтернету, щоб отримати доступ до різних сервісів (у випадку з ZigBee, наприклад, для доступу в інтернет буде потрібно використовувати прилад, який би виконував роль IP-шлюзу). Взаємодія з IP-мережами гарантується завдяки підтримки стандарту 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks), технології взаємодії по протоколу IPv6 поверх сіток стандарту IEEE 802.15.4. Це вважається одною з провідних переваг Thread в порівнянні з ZigBee. Завдяки цьому Thread ще містить деякі значущі функції, важкодоступні для ZigBee, в тому числі безпечне додавання нового приладу в мережу.

Thread стандартизує процес додавання приладів в мережу, примушуючи виробників додавати до власних продуктів цифрові мітки з кодом, які пізніше застосовуються кінцевими користувачами під час додавання. Це, мабуть, не комфортна процедура, але вона гарантує створення мережі більш безпечним і керованим ходом. Погодьтеся, в роботі з мережами на основі стандарту 802.15.14 це унікальність.

3.4.2 Недоліки технології Thread

З'явившись на ринку домашньої автоматизації набагато пізніше власних провідних суперників, Thread зобов'язаний був запропонувати користувачам справді щось унікальне, щоб відвоювати частку ринку у конкурентних технологій. Ці

протоколи, як ZigBee або ж Z-Wave розвивалися більше 10 років і мають велику кількість прихильників. У підсумку на їх основі зроблені сертифіковані компоненти, щоб забезпечити безпроводову асоціацію для млн. товарів, які вже присутні в експлуатації. Thread Group офіційно оголосила про Thread в липні 2015 року, а програма сертифікації анонсована в листопаді того ж року. Незабаром передбачалося виникнення 1 хвили Thread-пристроїв. Втім у 2018 році цих товарів на ринку було помічено не сотні і навіть і не десятки. А всього-то два. Власне що ще гірше, вони не пройшли повноцінну сертифікацію Thread. Абсолютно не так давно Thread Group розширила програму випробування, підключивши позначення Thread Ready для певних програм. І обидві продуктивні новинки заявлені всього лише як "Thread Ready" (готові до Thread).

Залежність від стандарту радіозв'язку IEEE 802.15.4 несе в собі ті ж труднощі, про які ми згадували під час обговорення ZigBee. Коли мережу Thread досягає обсягів орієнтовно в 200 вузлів, вона робиться наднасиченою в тому числі і в умовах, приблизних до ідеалу (тобто при повній недоступності в радіусі дії завад від інших приладів, що працюють в цьому ж діапазоні). Дана «хвороба» лімітування по масштабованості і працюючим частотам, властива для більшості представлених на ринку стандартів домашньої автоматизації, не може не розчаровувати. Тим більше враховуючи тот факт, власне що Thread дебютував на ринку більше ніж десяти роками пізніше, ніж його головні суперники. Крім того, ми зобов'язані згадати, що, як і ZigBee Alliance, галузеви консорціум Thread Group не містить прямого контролю над стандартом 802.15.4, який підтримується і розвивається тільки організацією IEEE.

Крок за кроком ми дісталися до верху моделі OSI - прикладного рівня. Thread залишає це місце абсолютно порожнім. В цьому випадку гостро постає питання, як Thread Group зможе вирішити проблему взаємної сумісності приладів. Як відомо, прикладний рівень вважається ключем до взаємодії, в наслідок цього без стандартизації на даному рівні окремі фреймворки додатків, підтримувані Thread, елементарно не зможуть спілкуватися між собою. І той факт, що Thread вважається стандартом на базі IP, також мало може допомогти. Само по собі включення до IP-

інтерфейсу гарантує безперебійну роботу лише тільки тоді, коли включення втілить в життя людина, яка може обрати ті інструменти, які підходять для певних справ. Прилади не можуть цього влаштувати автономно, і в наслідок цього не здатні комунікувати один з одним, в разі якщо їм не надані чіткі правила про те, як здійснити цей процес. Це як раз те, для чого і потрібен прикладний рівень.

Таблиця 3.4 – Переваги та недоліки Thread

Переваги	Недоліки
Відмовостійкість завдяки комірчастій топології мережі	Потенційні проблеми з сумісністю пристроїв різних виробників через відсутність стандартизації на прикладному рівні моделі OSI
Підтримка IP-протоколу забезпечує легкість підключення	Вкрай повільні темпи впровадження технології. За три роки створено всього два сертифікованих пристрої з підтримкою Thread.
Низький рівень споживання енергії	Погана стійкість через використання діапазону 2,4 ГГц
	Невизначені перспективи розвитку, оскільки консорціум Thread Group не впливає на розробку стандарту IEEE 802.15.4

Є ще один важливий момент, який треба згадати щодо самого верхнього рівня моделі OSI. Протоколи зв'язку, які визначають прикладний рівень, ще визначають процес співпраці між різними компаніями, що використовують певну технологію. Це означає, власне що виробник, наприклад, диммерів освітлення Z-Wave не зобов'язаний укладати будь-які договори з виробником ламп з вбудованими модулями Z-Wave, щоб відпустити на ринок контролер, керуючий цими лампами.

Вирішуючи застосувати Z-Wave, будь-який виробник автоматично дає згоду стати частиною великої екосистеми, в якій прилади різних постачальників взаємодіють без якихось юридичних і технічних обмежень. Thread не визначає прикладний рівень і критерії для зв'язку між приладами, в наслідок цього відсутня будь-яка нормативна основа для забезпечення можливої сумісності продуктів різних виробників.

3.5 Bluetooth Low Energy в моделі OSI

Як і Z-Wave, Bluetooth охоплює всі рівні провідної моделі OSI - від фізичного значення до прикладного. Цим чином, Bluetooth Special Interest Group (SIG), орган, який тримає під контролем розробку і ліцензування Bluetooth, містить цю ж рідкісну перевагу, як і Z-Wave Alliance, - прямо і автономно вносити всілякі конфігурації в стандарт.

Bluetooth Low Energy, як і інші стандарти зв'язку з невисоким енергоспоживанням і невисокою пропускнуою спроможністю, націлений на передачу даних маленькими пакетами і короткий час роботи приладу на батарейках в активному режимі. Якраз в даному ховається його провідна відмінність від звичайного нам традиційного Bluetooth, наприклад як приладу Bluetooth Low Energy об'єднуються один з одним лише тільки при потребі відправки або ж отримання даних.

На прикладному рівні взаємодія між рішеннями від різних виробників гарантується методом визначення профілів (специфікації роботи приладів з невисоким енергоспоживанням і певних програм). Цей принцип був запозичені з початкової специфікації традиційного Bluetooth. Цим чином, виробники можуть вводити потрібні їм профілі у власні прилади, забезпечуючи його сумісність з іншими продуктами Bluetooth Smart, що підтримують ту ж специфікацію. Відзначимо ще, власне що ймовірність імплантувати в рішення кілька профілів дозволяє виробникам гнучко коригувати працездатність власних товарів. Втім,

рішення від різних виробників зуміють повноцінно спілкуватися лише тільки в тому разі, коли у них є хоча б один спільний профіль.

3.5.1 Переваги Bluetooth Low Energy

Для технології, спрямованої на невисоке енергоспоживання, Bluetooth Low Energy володіє досить вражаючою швидкістю передачі даних - до 1 Мбіт / с (для нової п'ятої версії Bluetooth це збільшено до 2 Мбіт / с). Чим швидше швидкість, тим більше інформації можливо передати за одиницю часу. А це означає, власне що передавач Bluetooth швидше звільнить радіоефір, знижуючи можливість появи колізій. Це містить надзвичайно вагоме значення при роботі в цьому надзавантаженому діапазоні частот, як 2,4 ГГц. Завдяки підтримці сплячих вузлів (пристрої, які проводять величезну частину часу неактивні, час від часу "прокидаються" на короткий час лише тільки для швидкого виконання свого завдання, а слідом за тим ще швидко повернуться в сплячий режим) Bluetooth Smart забезпечує достійне, хоч і не одне з кращих в галузі термін служби батареї, дозволяючи конкретним датчикам і перемикачам працювати більше року від крихітних батарейок-таблеток. Власне що стосується такого критично актуального параметра для ринку домашньої автоматизації, як час резонансу приладу, то і тут BLE показує підсумки на рівні популярних технологій.

Крім того, Bluetooth Smart містить захоплюючу функцію, якої немає у інших розглянутих нами технологій. Це наприклад іменовані маячки (beacons). Застосовуючи функцію визначення близькості Bluetooth, маячки можуть змусити телефони виконувати конкретні дії, коли користувач знаходиться поблизу з ними. Маячки дають можливість ввести розмашистий діапазон оригінальних додатків: від push-повідомлень на базі визначення розташування до пропозицій чіткого позиціонування. Власне що особливо важливо, наприклад це те, що додавання кількох рядків коду в програмний стек - це все, власне що потрібно для обладнання розумного приладу за допомогою Bluetooth функціональністю маячка.

Функції, що базуються на здатності визначення близькості приладів Bluetooth, можливі тільки лише завдяки тому, що розумний прилад і телефон можуть прямо з'єднатися один з одним. І це сама величезна конкурентна перевага Bluetooth. З усіх технологій безпроводового зв'язку, що застосовуються в IoT, лише тільки Bluetooth і Wi-Fi на початку підтримуються буквально всіма телефонами, планшетами та ноутбуками на ринку. Але, крім того, власне що Wi-Fi не підходить для переважної більшості додатків інтернет речей, він орієнтує всі повідомлення крізь центральну точку доступу. І лише тільки Bluetooth забезпечує прямий зв'язок між телефонним апаратом і пристроєм. З точки зору користувача - це значна перевага, коли треба лише тільки особливий додаток, щоб його девайс став «віддаленим дисплеєм» для розумної домашньої мережі розумних приладів. Крім того, ця топологія важливо спрощує додавання нових конструкцій в існуючу мережу. З підтримкою Bluetooth вся процедура має можливість бути максимально полегшена, інстинктивно зрозуміла і безпечна.

3.5.2 Недоліки технології Bluetooth Low Energy

Bluetooth користується тим же діапазоном 2,4 ГГц, власне що і багато інших радіотехнологій, охоплюючи не тільки лише вже згадані нами Wi-Fi, ZigBee і Thread, а й велику кількість інших приладів, таких як мікрохвильові печі, радіоняні або ж безпроводові телефонні апарати. Не звертаючи уваги на те, власне що Bluetooth забезпечений конкретним інструментарієм для протидії завад (в тому числі, наприклад, технологією адаптивної зміни частоти, яка гарантує дієздатність в ході передачі даних динамічно перемикається між 40 іншими каналами, уникаючи найбільш гучних і завантажених), впровадження смуги частот 2,4 ГГц - це безперечний мінус. Так як, крім присутності незмінних завад, у спектра 2,4 ГГц є ще один величезний дефект - сигнал на даній частоті загасає набагато швидше, ніж на частотах менше 1 ГГц, коли радіохвилі проходять через стінки і інші завади, охоплюючи в тому числі і людський організм.

З цієї ж підстави радіус дії технології Bluetooth Low Energy не рахується її міцною стороною. Не звертаючи уваги на теоретичному рівні досяжність «до 100 метрів в зоні прямої видимості», для Bluetooth 4 версії при роботі 2-ух приладів в приміщенні ви можливо зможете планувати на відстань до 10 метрів. Негаразди додає і той факт, власне що дана цифра коригується в залежності не лише тільки від завад, які стануть перебувати на шляху поширення сигналу, але і опцій виробників, наприклад як з Bluetooth Smart у них є ймовірність в конкретних межах коригувати потужність сигналу приладу (в тому ж числі нарощувати його потужність і збільшувати енергоспоживання). Ключовий дефект Bluetooth Low Energy - конкурентність за спектр частот 2,4 ГГц з Wi-Fi, Zigbee, мікрохвильовими печами, радіонянями та іншої споживчою електронікою.

Є першопричина, по якій Bluetooth Smart, навмисне створений для укладення завдань стрімко зростаючого ринку IoT, буквально ні разу не розглядається як варіант для важких IoT-реалізацій, в тому числі і для зведення розгалужених мереж домашньої автоматизації. Справа в тому, власне що він був спроектований для підтримки порівняно нескладних сіток з топологією "зірка". Вона погано підходить для створення динамічного, керованого датчиками гнучкого і надійного середовища, яке ми хотіли б бачити в наших розумних оселях. Mesh-мережа вважається необхідною топологією для численних додатків, тим більше тих, які вимагають розширеного спектру або ж рівноправної комунікації між приладами. В наслідок цього не дивно, власне що всі відомі протоколи в категорії з невисокою пропускнуою спроможністю (Z-Wave і ZigBee) маршрутизують повідомлення крізь пористі мережі. Bluetooth ж, за рідкими винятками, вираженими в декількох пропрієтарних рішеннях (які, до того ж, несумісні між собою), цю можливість не надавав.

Таблиця 3.5 – Переваги та недоліки Bluetooth Low Energy

Переваги	Недоліки
Висока швидкість передачі даних в мережі	Погана завадозахищеність в перевантаженому діапазоні частот 2,4 ГГц
Помірне енергоспоживання в порівнянні з Wi-Fi	Недостатня надійність: не використовується топологія пористих мереж (можливо, з поширенням технології лавинної маршрутизації цей недолік буде усунений в нових моделях пристроїв)
Хороша сумісність: охоплені всі рівні моделі OSI	Малий практичний радіус дії (максимум до 10 м в приміщеннях). Топологія "зірка" не дозволяє розширювати мережу за допомогою ретрансляторів. Можливо, з поширенням технології лавинної маршрутизації цей недолік буде усунений в нових моделях пристроїв

Висновки до розділу

Дослідивши переваги та недоліки кожної із технологій можна зробити висновок що найдосконалішим є протокол Z-Wave.

В технологіях ZigBEE та Wi-Fi проблемна сторона – це безпека.

Усі протоколи показали результат низького енергоспоживання окрім Wi-Fi. Цей протокол можна відмітити як ненадійніший серед розглянутих.

ВИСНОВКИ

На підґрунті аналізу та дослідженні безпроводових технологій отримано такий результат:

- 1) Технологія Wi-Fi має ряд позитивних сторін, вона поширена в комп'ютерах і мобільних пристроях, забезпечує високу швидкість передачі даних і має велику площу дії, але за великою кількістю недоліків, а саме високе енергоспоживання, несумісність багатьох пристроїв, проблемою інформаційної безпеки та проблемою додавання пристроїв у систему робить цю технологію ненадійною.
- 2) Thread порівняно з Wi-Fi вирішила проблему з енергоспоживанням та легкістю додавання пристроїв але використовуючи частотний діапазон 2.4 ГГц має погану стійкість, що дуже важливо для системи розумного будинку в цілому. Також із-за поганого впровадження технології створено дуже мало сертифікованих пристроїв, що ставить під питання технологію як вибір домашньої автоматизації.
- 3) BLE має також низький рівень енергоспоживання, але вона має малу завадозахищеність. Як ми вже розглянули частотний діапазон 2,4 ГГц не є досконалим, тому технологію можна вважати досить ненадійною, оскільки є ризик втрати сумісності між розумними пристроями і як наслідок – ненормована робота системи.
- 4) Протокол ZigBEE на фоні вище розглянутих технологій буде переважно кращим, але також через використання частотного діапазону 2,4 ГГц велика ймовірність завад, особливо створюваних, якщо є мікрохвильова піч та на фоні використовуються технології Wi-Fi та Bluetooth. Її сміливо можна вважати ненадійною із за відсутності жорстких умов сертифікації. Таким чином виробники розумних пристроїв для цієї технології можуть знехтувати питанням безпеки та шифруванням даних.

- 5) Найкращою та найдосконалішою виявилася технологія Z-Wave. Вона має чудову систему безпеки завдяки протоколам S2 та має високу стійкість, тому що захищена від впливу інших пристроїв Wi-Fi, Bluetooth, мікрохвильових печей та іншого обладнання, що працює в діапазоні 2,4 ГГц. Чудова сумісність пристроїв завдяки умовам сертифікації. Єдиний недолік цієї технології – це те, що вона використовує різний частотний діапазон в залежності від країни. Це пояснюється зайнятістю смуг іншими технологіями, які реалізуються у мережі. Це може виразитися на підборі розумних пристроїв для системи. Але приділяючи увагу і підбираючи вірні пристрої, ця технологія стане найкращим та найнадійнішим вибором для системи розумного будинку.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Thread Vs. ZigBee (For IoT Engineers) URL: <https://www.link-labs.com/blog/thread-vs-zigbee-for-iot-engineers> (дата звернення 16.03.2020).
2. Thread URL: <https://iot.ru/wiki/thread> (дата звернення 16.03.2020).
3. Bill Rose, Home Networks: A Standards Perspective (IEEE Communication Magazine, Dec. 2001).
4. Беспроводные сети ZigBee и Thread URL: <http://www.wless.ru/technology/?tech=1> (дата звернення 18.03.2020).
5. S. Daniel Park, Things to think about when Interworking 6LoWPAN and Zigbee networks (December 2005, IETF draft name: draft-daniel-6lowpan-zigbee-issues-00)
6. Основы Bluetooth Low Energy URL: <https://www.rlocman.ru/review/article.html?di=183939> (дата звернення 06.04.2020)
7. Наукові записки Українського науково-дослідного інституту зв'язку. – 2016. – №2(42)
8. Yang, L. (2012) Design of Monitoring and Controlling System of Smart Home based on ZigBee. Master's Thesis, Beijing Jiaotong University, Beijing.
9. Ruan, X. (2010) Analysis and Comparison of Several Smart Home Wireless Networking Technology. Science & Technology Information, 27, 39-42.
10. Liu, Y. Study on smart home system based on internet of things technology. In Informatics and Management Science IV; Du, W., Ed.; Springer: London, UK, 2013; Volume 207, pp. 73–81.
11. Bluetooth Low Energy-based Smart Home Android Solution URL: <https://ieeexplore.ieee.org/document/8861866> (дата звернення 06.05.2020).
12. IEEE. IEEE Standard for Information Technology-Telecommunications and Information Exchange between Systems-Local and Metropolitan Area Networks-Specific Requirements Part 15.4: Wireless Medium Access Control (MAC) and

- Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs); Technical Report; IEEE: New York, NY, USA, 2006.
13. Tompros, S.; Mouratidis, N.; Draaijer, M.; Foglar, A.; Hrasnica, H. Enabling applicability of energy saving applications on the appliances of the home environment. *IEEE Netw.* 2009, 23, 8–16.
 30. Zadeh, L.A. The concept of a linguistic variable and its application to approximate reasoning—II. *Inf. Sci.* 1975, 301–357.
 14. Adams, C. E. (2002). Home area network technologies. *BT Technology Journal*, 20(2), 53–72.
 15. Valtchev, D., & Frankov, I., & ProSyst Software AG. (2002). Service Gateway Architecture for a Smart Home. *IEEE Communications Magazine*, 126–132.
 16. F. Liu and H. Zhao, "The Design of WIFI-Based Smart Home Communication Hardware Adapter," 2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC), Qinhuangdao, 2015, pp. 1193-1197.
 17. H. Jiang, B. Liu and C. W. Chen, "Performance analysis for ZigBee under WiFi interference in smart home," 2017 IEEE International Conference on Communications (ICC), Paris, 2017, pp. 1-6.

ДОДАТОК А

SUMMARY

A smart home is becoming a reality today.

It is an automated home with devices that are connected to each other and that can be controlled on the home dashboard or via a smartphone via the Internet. But until recently, SmartHome has always remained a high market or a platform for several amateurs and early innovators.

The potential of home automation in the mass market has long been recognized, and finally today we see the beginning of a new era when many large operators, service providers and utilities are launching SmartHome programs. They can be controlled via a TV device or gateway via the Internet, which allows subscribers to turn their homes into state-of-the-art machines that can be tracked and monitored from anywhere in the world using smartphones, tablets or mobile devices.

Operators are starting to offer SmartHome applications as an additional service to their current offerings of television, telephone services, Internet and entertainment; their customers can choose from applications that meet their specific needs. The owner of one house has different requirements to make his house smarter than the elderly or a family with children. These programs can check and control "things at home", such as temperature control (changing the thermostat setting), security (make sure the door is locked), alarm (sensors and cameras) or energy management (eg lighting control) and health monitoring. me and the condition of the elderly. For all these different programs to be compatible, they all need to be able to interact with each other.

The protocol is a set rules that allow two or more devices on the network to enter a reliable association and securely exchange data with each other. In order for a smart home to become a reality, a large share of communications must be wireless.

Different wireless technologies have been developed to perform different tasks. Accordingly, they do their own work in different ways. Almost all the nuances will be

indisputable, if you consider these network technologies through the prism of the reference model OSI.

The International Organization for Standardization (ISO) came up with a model of Open Systems Interconnection (OSI) in the 80s of last century. OSI is the basis for coordinating the development of communication stereotypes and still remains the reference model for communication networks. The OSI design evaluates the process of communication in the network as a managed hierarchy consisting of 7 values. Each of them is responsible for specific functions and solves clearly specific tasks within the 1st value, as well as interaction with the levels located just below and above.

Thanks to the constant improvement of technology, people are more comfortable living

At home and more convenient and safer. Currently, the trend of smart home - from centralized control to distributed control. Currently, four main wireless technologies are used in a smart home: Bluetooth, WiFi, Z-Wave, Zig-bee. WiFi and Zig-bee technology are the most competitive.

Wi-Fi development is based on IEEE 802.11x wireless networking standards. They define only the 1st and 2nd level of the OSI model - material and channel. The Wi-Fi network contains a "star" topology, which means that all its nodes are combined with a central component - a wireless router. In such a topology, end devices can be added and removed from the network, which does not affect the unity of its structure and data transmission in it.

Actually, as for the network and transport values, for their Wi-Fi usually uses other normal protocols - UDP or TCP for the transport value, and IPv4 or IPv6 for the network value. And the application level, which, as we already know, is responsible for the compatibility of devices, is not defined decisively, and is entirely left to the manufacturers of software and hardware conclusions.

Zigbee communication is specially built for control networks and sensors according to the IEEE 802.15.4 standard for wireless personal networks (WPAN), and it is a product from the Zigbee alliance. This communication standard defines the physical and control levels of media access (MAC) for processing many low-speed devices.

These ZigBee WPANs operate at 868 MHz, 902-928 MHz and 2.4 GHz. The 250 kbps data rate is best suited for intermittent as well as intermediate two-way data transfer between sensors and controllers.

Zigbee is an inexpensive and low-power network, widely deployed for program control and monitoring, where it covers 10-100 meters within range. This communication system is cheaper and simpler than other proprietary wireless sensor networks, such as Bluetooth and Wi-Fi.

The Zigbee can operate in a variety of modes, saving battery power. Zigbee networks are expanding with the use of routers and allow many nodes to connect to build a wider area network.

Any regular Z-Wave network has the ability to support up to 232 devices. When it is necessary to include the largest number of devices, the combination of grids is used. A number of Z-Wave grids can be used seamlessly in one system without interfering with each other. This is achieved by minimizing the volume of the transmitted packet and the mandatory requirement for a small load on the radio channel, which requires the device to be in a state of transmission for a maximum of 1% of the time. However, the nodes of different grids do not have the ability to "see" each other and, accordingly, to communicate with each other in any way. Communication between networks is performed through devices that act as network bridges.

Devices in the same network can exchange information with each other, including when outside the line of sight. In this case, the device uses intermediate nodes (other devices in the same network, not counting those that are battery-powered and most of the time work in "sleep" mode due to battery savings) to transmit information to other devices when they are outside the range of the first device.

Bluetooth Low Energy, like other communication standards with low power consumption and low bandwidth, aims to transmit data in small packets and short battery life of the device in active mode. This is where its leading difference from the usual traditional Bluetooth lies, for example, as a Bluetooth Low Energy device is combined with each other only when you need to send or receive data.

At the application level, the interaction between solutions from different manufacturers is guaranteed by the method of determining profiles (specifications for the operation of low-power devices and certain programs). This principle was borrowed from the original specification of traditional Bluetooth. This allows manufacturers to incorporate the profiles they need into their devices, ensuring that it is compatible with other Bluetooth Smart products that support the same specification. Note also that the probability of implanting several profiles in the solution allows manufacturers to flexibly adjust the performance of their products. However, solutions from different manufacturers will be able to fully communicate only if they have at least one common profile.